Australian Government
Department of Defence
Defence Science and
Technology Organisation

A Network Centric Warfare (NCW) Compliance Process for Australian Defence

Michele Knight, Les Vencel and Terry Moon

Intelligence, Surveillance and Reconnaissance Division and
Defence Systems Analysis Division
Defence Science and Technology Organisation

DSTO-TR-1928

ABSTRACT

The NCW Program Office (NCWPO) is responsible for ensuring that the ADF's capability projects are Network Centric Warfare (NCW) compliant, from the time they are listed in the Defence Capability Plan until they enter service as realised capabilities and throughout life-of-type. The NCWPO has engaged a number of different groups to look at the problem of NCW Compliance from different perspectives. This report describes one of these studies. It proposes an NCW Compliance Process that is based on a simple underlying conceptual model. It also identifies some critical issues to be addressed by the NCWPO in order to improve the rigour and quality of the NCW Compliance Process.

This work was done under the auspices of the DSTO NCW S&T Initiative.

Produced by

DSTO *Defence Science and Technology Organisation*
PO Box 1500
Edinburgh South Australia 5111 Australia

Telephone: (08) 8259 5555
Fax: (08) 8259 6567

AR-013-770
August 2006

APPROVED FOR PUBLIC RELEASE

A Network Centric Warfare (NCW) Compliance Process for Australian Defence

Executive Summary

The Australian Defence Force (ADF) is moving towards implementation of Network Centric Warfare (NCW) concepts. The NCW Program Office (NCWPO) is responsible for ensuring that the ADF's capability projects are 'NCW compliant, from the time they are listed in the DCP until they enter service as realised capabilities and throughout life-of-type' [DCOP 2006]. The NCWPO has engaged a number of different groups to look at the problem of NCW Compliance from different perspectives. This report describes one of these studies.

This report proposes an NCW Compliance Process that is based on a simple underlying conceptual model. The process may be used to check that the ADF's capability projects have addressed NCW-related issues at each stage of the Defence Capability Development Process [DCOP 2006]. To guide this study, the NCWPO developed the following objective for the NCW Compliance Process:

> *To ensure the ADO's Capability Development Process delivers projects that are integrated in support of Australia's future warfighting capability requirements.*

This document provides an overview of the proposed NCW Compliance Process, a detailed Process Model and Compliance Question List for subsequent implementation. It also identifies the following critical issues to be addressed by the NCWPO in order to improve the rigour and quality of the NCW Compliance Process:

1. Systems and Operations Analysis effort to translate the ADO's NCW guidance for the whole-of-force into Netforce principles and target states that can be checked for individual projects
2. Development of an Australian Netforce Design and supporting Technical Reference Model
3. An assessment of the case for Services-Oriented Architectures for the ADO
4. Development of an architecture schema for the current and future ADO
5. Compliance with CDG mandates for Capability Project Documentation
6. Establishment of an NCWPO Support Team with an appropriate skills profile.

The NCW Compliance Process should be updated as these issues are addressed, and in response to feedback from both the NCWPO Support Team and desk officers who use the process. It is recommended that the NCW Compliance Process should be reviewed in line with updates to the Defence Capability Development Manual.

The proposed NCW Compliance Process includes compliance checks conducted at the First Pass, Second Pass and Acquisition stages of the Defence Capability Development Process (Figure 1). Note: the Acquisition stage of the NCW compliance process is still to be developed.

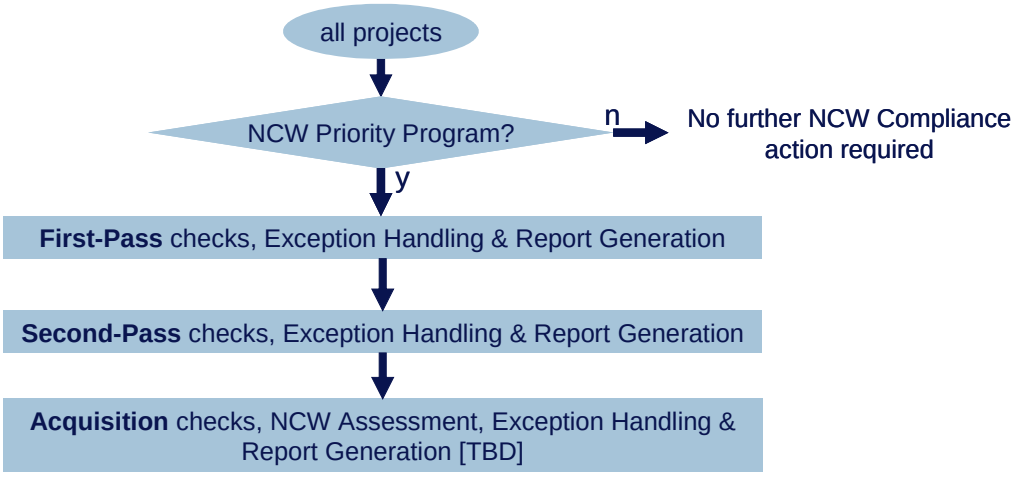


Figure E1 NCW Compliance Process Overview

The proposed NCW Compliance Process includes seven components, three of which are still to be developed. Each component may be applied at the First Pass, Second Pass and Acquisition stage of the Defence Capability Development Process (Figure 2). For most of the components, the level of detail will tend to increase at later stages, reflecting the increase in detail and maturity of project documentation as the project progresses through the Defence Capability Development Process.

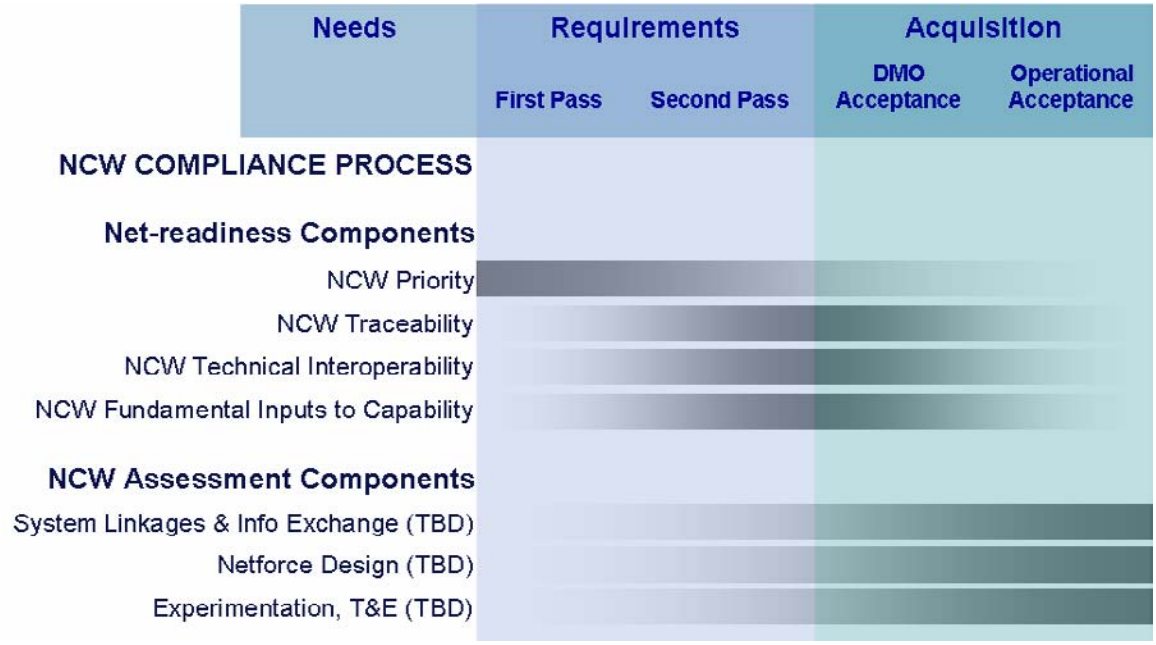


Figure E2 NCW Compliance Process Alignment with Capability Development Process

The distinctive feature of the proposed NCW Compliance approach is the premise that a capability project will not exhibit net-centric behaviour until it is connected as part of an NCW System of Systems or *Netforce*. Therefore NCW compliance should be checked in three stages:

1. Is the capability project ready and able to be connected as part of a Netforce? This requires standards-based checks for *Net-readiness*.
2. What behaviour will it exhibit as part of that Netforce? This requires assessment of the capability project as part of a Netforce system of systems.
3. Will the Netforce support ADO missions and objectives? This requires assessment of the Netforce system of systems.

The proposed NCW Compliance Components are summarised in the following table.

Table E1 NCW Compliance Components

Net-Readiness Components	
NCW Priority	Checks whether the project is (or should be) included in the NCW Roadmap and Integration Plan. This component is used as a filter, to identify projects that need to be checked for NCW compliance.
Fundamental Inputs to Capability (FIC)	Ensures that the project has identified and addressed the impact of NCW Compliance on FIC elements.
NCW Traceability	Ensures that the project's design and documentation support NCW guidance and provide a traceable path from NCW guidance to operational activities, system functions and services and then to the necessary technical standards.
Technical Interoperability	Ensures that the project complies with agreed technical standards for data, information and network interoperability.
Netforce Assessment Components	
System Linkages and Information Exchanges (to be developed)	Will be used to identify legacy and future systems that will need to exchange information with the project under assessment. This component could also be used to prioritise legacy systems for which a wrapper should be developed to enable interfacing to the Netforce.
Netforce Design Component (to be developed)	Will be used to ensure that projects are consistent with Netforce design attributes, e.g. architecturally and functionally consistent.
NCW Experimentation and T&E Component (to be developed)	Will be used to test and assess the delivered capability's behaviour in a Netforce environment.

This report delivers the Net-readiness components of the NCW Compliance Process. It is recommended that additional work should be undertaken to develop the Assessment components of the NCW Compliance Process, which will focus on assessing the capability of Net-ready projects to operate in a Netforce environment.

Authors

Michele Knight

Intelligence, Surveillance & Reconnaissance Division

Michele Knight joined DSTO in 1991, with a Bachelor of Electrical & Electronic Engineering from the University of Western Australia. The main focus of her work is in applying systems engineering and operational analysis techniques to the study of Defence Intelligence, Surveillance and Reconnaissance (ISR) systems. Michele is currently studying for a Masters in Defence Operations Research.

Les Vencel

VCORP Consulting P/L

Les Vencel has around thirty years experience in the engineering and management of Defence systems projects, both from within the government as well as in industry. He is currently the principal systems consultant and director of VCORP Consulting Pty Ltd. His prior experience comprises senior engineering and management roles in industry ranging from General Manager of the Radar Systems division of GEC Marconi Systems, senior manager on Australia's JORN radar program to over 15 years experience in the Defence Science and Technology Organisation. At DSTO, he was primarily involved in radar and avionics systems with the F/A-18 and the F-111C. His last position, prior to leaving the DSTO, was Head of the Hornet Radar Systems Group. Mr. Vencel's primary work interests are the application of systems engineering to complex and evolutionary programs. He has degrees in Mathematical Science and Electrical Engineering from the University of Adelaide and is currently undertaking his doctorate in Systems Engineering.

Terry Moon

Defence Systems Analysis Division

Terry Moon obtained his BSc (Hons) from Monash University in 1975, MSc from the University of Melbourne in 1979 and PhD from Monash University in 1984. He has over 30 years experience in research having worked in astronomy and astrophysics, solar energy technology and Defence Science. Since joining the DSTO in 1986, Terry has worked in the fields of electronic warfare technology, program evaluation, operations analysis, imaging radar, systems analysis, capability engineering and network-centric warfare. He has worked on a number of major Australian Defence projects and studies including field trials of the Nulka decoy, the Wide Area Surveillance Study, the project definition phase of Project AIR 87 and the risk mitigation phase of Project JP 129. Terry is currently Head NCW Strategic Initiative.

Contents

Glossary

ADF	Australian Defence Force
ADO	Australian Defence Organisation
ATSL	Australian Technical Standards List
C3	Command, Control and Communications
C3I	Command, Control, Communications and Information
CASE	Computer Aided Software Engineering
CDG	Capability Development Group
CV	Common View (see Defence Architecture Framework)
DAF	Defence Architecture Framework A framework depicting the Australian Defence methodology for the production of Enterprise Architecture (EA) data and products. The DAF products include Common Views (CV), Operational Views (OV), System Views (SV) and Technical Views (TV). There are 10 essential views and 18 supporting views: CV-1 (Essential) Overview and Summary Information CV-2 (Essential) Integrated Dictionary CV-3 (Supporting) Capability Maturity Profile CV-4 (Essential) Architecture Compliance Statement OV-1 (Essential) High-level Operational Concept Graphic OV-2 (Essential) Operational Node Connectivity Description OV-3 (Essential) Operational Information Exchange Matrix OV-4 (Essential) Command Relationship Chart OV-5 (Essential) Activity Model OV-6a (Supporting) Operational Rules Model OV-6b (Supporting) Operational State Transition Description OV-6c (Supporting) Operational Event/Trace Description OV-7 (Supporting) Logical Data Model SV-1 (Essential) System Interface Description SV-2 (Supporting) Systems Communications Description SV-3 (Supporting) Systems to Systems Matrix SV-4 (Supporting) Systems Functionality Description SV-5 (Supporting) Operational Activity to System Function Traceability Matrix SV-6 (Supporting) System Data Exchange Matrix SV-7 (Supporting) System Performance Parameters Matrix SV-8 (Supporting) System Evolution Description SV-9 (Supporting) System Technology Forecast SV-10a (Supporting) Systems Rules Model SV-10b (Supporting) Systems State Transition Description SV-10c (Supporting) Systems Event/Trace Description SV-11 (Supporting) Physical Data Model TV-1 (Essential) Technical Architecture Profile TV-2 (Supporting) Standards Technology Forecast
DCC	Defence Capability Committee
DCP	Defence Capability Plan
DHA	Defence Housing Authority
DIE	Defence Information Environment
DMO	Defence Materiel Organisation
DoD	Department of Defence
DSTO	Defence Science and Technology Organisation

EA	Enterprise Architecture (also see Defence Architecture Framework) The Defence Enterprise Architecture is comprised of six component architectures: 1. Business: this defines the business strategy, governance, organisation, and key business processes; 2. Information: this describes the structure of the logical and physical data assets and data management resources; 3. Systems (applications): this describes the applications (systems) to be deployed, their interactions, and their relationships to Defence processes; 4. Infrastructure architecture: the infrastructure intended to support the deployment of core, mission-critical applications; 5. Standards: this defines the standards that are applied to the first four EA components; and 6. Security: this defines security related policies, processes, procedures and doctrine to be applied to the first five EA components.
FIC	Fundamental Inputs to Capability The FIC are a guide that may be used to quantify capability. The eight FIC are Organisation, Personnel, Collective Training, Supplies, Facilities, Major Systems, Support and Command & Management.
First Pass	Part of the Defence Capability Development Process. First Pass Approval allocates funds from the Capital Investment Program to enable the options endorsed by Government to be investigated in further detail, with an emphasis on detailed cost and risk analysis. The process gives Government the opportunity to narrow the alternatives being examined by Defence to meet an agreed capability gap.
FPS	Function and Performance Specification
GIG	Global Information Grid The GIG is the organising and transforming construct for managing information technology (IT) throughout the US Department of Defense. The GIG vision is to empower users through easy access to information anytime and anyplace, under any conditions, with attendant security.
ISO	International Standards Organisation (see OSI Reference Model)
IT	Information Technology
JCSE	Joint Command Support Environment
JORN	JINDALEE Operational Radar Network
JTA	Joint Technical Architecture (US Technical Reference Model, now superseded by the NCOW RM)
JTF	Joint Task Force
LISI	Levels of Information Systems Interoperability (LISI) Maturity Model provides the US DoD with a common basis for requirements definition and for incremental system improvements (C4ISRAFWG 1998). The model defines five levels of capability maturity for each of four attributes: – Procedures – Applications – Infrastructure (hardware, communications, security, and system services) – Data The five levels are: Level 4: Enterprise – Interactive manipulation; Shared Data and applications Level 3: Domain – Shared data; "Separate" applications Level 2: Functional – Minimal common functions; Separate data and applications Level 1: Connected – Electronic connection; Separate data and applications Level 0: Isolated – Non-connected, manual gateways

MoD	(UK) Ministry of Defence
NATO	North Atlantic Treaty Organisation
NBD	Network Based Defence (Sweden)
NCO	Network Centric Operations
NCOW RM	Net Centric Operations and Warfare Reference Model The current (2006) US Defense Technical Reference Model. It is an architecture-based description of activities, services, technologies, and concepts that enable a net-centric enterprise information environment for warfighting, business, and management operations throughout the US Department of Defense.
NCSP	NATO C3 Common Standards Profile The NCSP specifies the minimum set of communication and information technology standards mandated for the acquisition of all NATO C3 systems
NCW	Network Centric Warfare
NCWPO	Network Centric Warfare Program Office
NCW Principles	The NCWPO is in the process of identifying a set of endorsed NCW Principles based on high-level policy guidance
NEC	Network-Enabled Capability (UK)
Netforce	An NCW system of systems: a group of capabilities configured into a force that exhibits desired NCW behaviour
Net-readiness	A capability project is net-ready if it is ready and able to be integrated as part of a Netforce system of systems: – the project complies with agreed standards – project documentation demonstrates support for endorsed NCW Principles – the project has made allowance for the impact of NCW compliance on the Fundamental Inputs to Capability (FIC) – the project complies with endorsed Netforce functional design principles
NJTF	Networked Joint Task Force
NPI	NCW Prioritisation and Integration
NRT	Near Real Time (see also Real Time) Pertaining to the timeliness of data or information that has been delayed by the time required for electronic communication and automatic data processing. This implies there are no significant delays.
OCD	Operational Concept Document
OCIO	Office of the Chief Information Officer
OSI	Open Systems Interconnection Refers to the OSI Reference Model, also known as the ISO/OSI seven layer model, developed by the International Standards Organisation (ISO). The seven layers are: 7 Application 6 Presentation 5 Session 4 Transport 3 Network 2 Data Link 1 Physical
OV	Operational View (see Defence Architecture Framework)
PGM	Precision-Guided Munitions
POL	Petrol, Oils and Lubricants
Quadripartite	Pertaining to the US, UK, Canada and Australia
RFP	Request for Proposal

RFT	Request for Tender
RM	Reference Model (see also Technical Reference Model)
RMR	Risk Mitigation Review
RT	Real Time (see also Near Real Time) The absence of delay in the detection, transmission and reception of data
Second Pass	Part of the Defence Capability Development Process. Second Pass is the final milestone in the Capability Development Process Requirements Phase, at which point Government will endorse a specific capability solution and approve funding for the Acquisition Phase. The project cannot proceed to the Acquisition Phase until Second Pass approval is obtained from Government.
SOA	Services-Oriented Architectures
SOS	System of Systems
SV	Systems View (see Defence Architecture Framework)
T&E	Test and Evaluation
TARDIS	Defence Capability Development Group's knowledge management system
TBD	To Be Developed
TCD	Test Concept Document
TIE	Tactical Information Exchange
Tolk	Refers to Andreas Tolk, author of the Reference Model for Measures of Merit for Coalition Interoperability [Tolk 2003]. This reference model proposes a layered framework for assessing interoperability. The layers are: – Political Objectives – Harmonized Strategy/Doctrines – Aligned Operations – Aligned Procedures – Knowledge/Awareness – Information Interoperability – Data/Object Model Interoperability – Protocol Interoperability – Physical Interoperability
TRM	Technical Reference Model A TRM describes the standards, specifications and technologies that support the delivery of capabilities
TV	Technical View (see Defence Architecture Framework)
UK	United Kingdom
US	United States [of America]

1. Introduction

The Australian Defence Force (ADF) is moving towards implementation of Network Centric Warfare (NCW) concepts. The NCW Program Office (NCWPO) is responsible for ensuring that the ADF's capability projects are 'NCW compliant, from the time they are listed in the DCP until they enter service as realised capabilities and throughout life-of-type' [DCOP 2006]. The NCWPO has engaged a number of different groups to look at the problem of NCW Compliance from different perspectives. This report describes one of these studies.

This report proposes an NCW Compliance Process that is based on a simple underlying conceptual model. The process may be used to check that the ADF's capability projects have addressed NCW-related issues at each stage of the Defence Capability Development Process [DCOP 2006]. To guide this study, the NCWPO developed the following objective for the NCW Compliance Process:

> *To ensure the ADO's Capability Development Process delivers projects that are integrated in support of Australia's future warfighting capability requirements.*

This report provides:

- An overview of the proposed NCW Compliance Process and its relationship to higher-level defence guidance and the Defence Capability Development Process
- A summary of further work that is still needed – in particular, expanding the compliance process to include an assessment of how each project will operate in an NCW environment
- An appendix summarising critical issues to be addressed by the NCWPO, including implementation issues
- Appendices containing more detailed discussion of the proposed NCW Compliance Process.

Definitions

NCW Principles	The NCWPO is in the process of identifying a set of endorsed NCW Principles based on high-level policy guidance
Netforce	An NCW system of systems: a group of capabilities configured into a force that exhibits desired NCW behaviour
Net-readiness	A capability project is net-ready if it is ready and able to be integrated as part of a Netforce: – the project complies with agreed standards – the project's documentation demonstrates support for endorsed NCW Principles – the project has made allowance for the impact of NCW compliance on the Fundamental Inputs to Capability (FIC) – the project complies with endorsed NCW (Netforce) functional design principles

2. Background

The US and UK have developed processes for checking the congruence of the characteristics of major military systems with the attributes desired for net-centric operations. The US has established a Net-Centric Checklist, the purpose of which is to '*assist program managers in understanding the net-centric attributes that their programs need to implement to move into the net-centric environment as part of a service-oriented architecture in the Global Information Grid*' [US CIO 2004]. The UK has taken a different approach in developing 'NEC Benefit Analysis' so as to understand the relationship between investment and force effectiveness [Dstl 2004, MoD 2005]. In both countries, the method for checking the congruence of military capabilities with net-centric attributes has been constructed with their capability development and acquisition processes in mind [Boyd et al 2005].

In Australia a team led by Dr Mark Unewisse (DSTO) developed a methodology for checking the state of NCW readiness in the Land Force and applied it successfully to a collection of capabilities known as LAND 5000. This has been recently expanded into a NCW Prioritisation and Integration (NPI) methodology used for detailed analysis of groups of projects or collections of capabilities. While useful for identifying cross-capability integration problems and risks, the NPI approach was not originally designed to check the compliance of individual projects [Boyd et al 2005]. Development of the NPI continues.

Another team led by Dr Gina Kingston (DSTO) has developed an NCW Risk Mitigation Review (RMR) Framework and applied it to a specific ADF Project. The RMR Framework is referenced to the Defence Capability Development Process and aims to determine 'the level of risk of a project not achieving a required level of NCW integration' [Richer et al 2006]. In the absence of an agreed NCW architecture or Technical Reference Model for Australian Defence, the RMR Framework may be used to assess cross-project interactions and the NCW characteristics of a project. When complete, the Framework will include an assessment of the project's Fundamental Inputs to Capability (FIC) [Kingston et al 2006].

The NCW Compliance Process proposed in this report is significantly different from the approach taken by Kingston et al [2006] and Richer et al [2006] in that it:

1. Is based on the model proposed by Keus [2005] rather than on the ISO, LISI and Tolk models [Kingston et al 2006];
2. Calls for the establishment of a Technical Reference Model with agreed standards, rather than allowing systems to evolve without strict adherence to standards;
3. Has a stated objective to 'ensure the ADO's Capability Development Process delivers projects that are integrated in support of Australia's future warfighting capability requirements' that is significantly different from the RMR Framework's stated NCW Compliance aim to 'facilitate communication and information sharing between the projects, optimising cross-project integration…' [Richer et al 2006, Presentation Slide 4]

3. NCW Compliance Approach

The NCW Compliance Process described in this report was developed by DSTO for the NCWPO in accordance with the following guiding principles:

- Based on an underpinning conceptual model
- Simple, objective and repeatable compliance checks
- Aligns with the Defence Capability Development Process
- NCW Compliance Process can be improved over time.

At the specific request of the NCWPO, the compliance process includes a FIC component.

3.1 Theoretical Basis

The foundational concepts of Network Centric Warfare are discussed at length by Alberts, Garstka & Stein [1999] and Alberts [2002]. Despite the subtle differences in the approaches taken by various countries, with a variety of terms such as NEC, NBD and NCO currently in use, they appear to have the same underlying aims. All of these net-centric approaches use information sharing to achieve better situational awareness, improved decision-making and enhanced collaboration across elements of a military force, resulting in self-synchronisation of those elements for decisive, swift, effective and efficient military outcomes.

Keus [2005] has made significant progress towards defining the properties of net-centric military forces and systems. Keus takes a Systems of Systems (SoS) approach and starts with the concept of providing adequate information for better situational awareness, self-synchronisation and enhanced collaboration. Keus introduces the Network-Node Paradigm: 'All entities in a net-centric operation can be regarded as nodes interacting with each other through a communications network.' This view is similar to that of McKenna et al. [2006] who treat net-centric military systems as 'a network of nodes and links where information is the key currency of exchange'.

Keus's [2005] SoS approach may be summarised as follows:

- An NCW System of Systems comprises a reconfigurable group of nodes, where each node performs one or more basic functions (collection, information processing, decision-making, communications, taking action, providing support);
- Each node has some elementary properties that enable it to be modelled and connected in an NCW environment. These properties are defined as identity, status, capability, structure, control, security, integration, interaction. For legacy systems, a wrapper is required to enable interfacing to the network;
- Higher-level capabilities (such as situation awareness, synchronised decision-making and engagement) emerge from the interactions between groups of nodes.

The NCW compliance approach described in this report is based on Keus's [2005] concept that NCW capabilities will emerge from the interactions between groups of nodes that are connected via a communications network. The distinctive feature of this compliance approach is the premise that a node (eg a capability project) will not exhibit net-centric

behaviour until it is connected as part of an NCW System of Systems or *Netforce*. Therefore NCW compliance should be checked in three stages:

1. Can the capability project (i.e. node) be connected as part of a Netforce?
2. What behaviour will it exhibit as part of that Netforce?
3. Will the Netforce support ADO missions and objectives?

3.2 NCW Enterprise Model

The NCW Compliance Process is based on a simple three-layer NCW Enterprise Model (Figure 1).

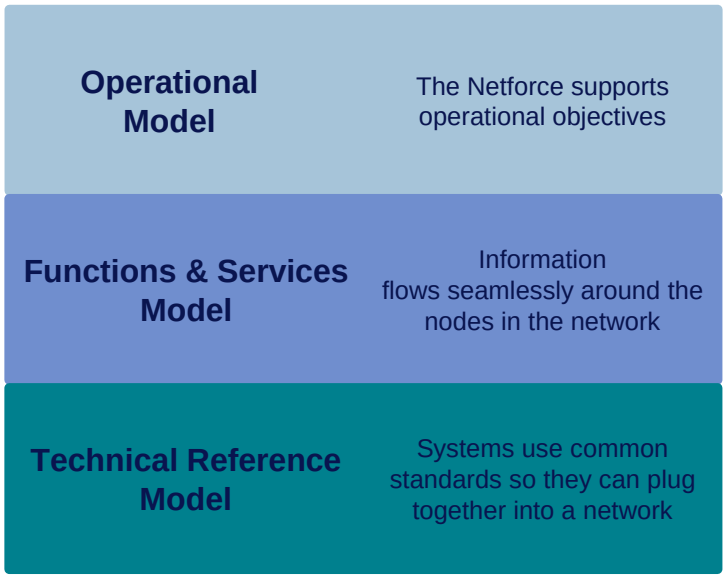


Figure 1 NCW Enterprise Model

The top layer represents the ADO's operational model and includes higher-level NCW policy guidance and force or mission objectives. The middle layer represents the essential functions and services (eg sensing, decision-making, tasking) that will provide the generic structures (eg sense-decide-act loops) and emergent properties (eg situational awareness) that support the NCW force objectives. The bottom layer is a Technical Reference Model (TRM) for the future force. Individual systems and projects that comply with the standards in the TRM will be compatible with one another, and therefore able to be connected more easily into useful functions and services structures.

A way to think of the enterprise model is that the TRM provides the enabling technical infrastructure that allows functions and services to be performed to permit operational activities to be undertaken in accordance with mission needs.

3.3 From high-level policy guidance to NCW Compliance

The NCW Roadmap [CDG 2005] outlines the ADF's future NCW capability requirements, the ADF's current NCW capabilities and how the ADF's future NCW capability requirements are to be realised. Systems and operations analysis is required to translate this NCW guidance for the whole-of-force into NCW principles and target states that can be used to develop an Australian NCW-capable force (or *Netforce*) Design[1]. An Australian Netforce Design would identify the architecture schema, characteristics and functional design attributes of a future Australian Netforce.

The requirement for NCW systems/operations analysis is flagged as a critical issue for the NCWPO to address (Appendix A – Critical Issues List).

3.4 Netforce Capability versus Project Net-Readiness

NCW guidance [CDG 2005] defines the aspirational NCW behaviour that would be exhibited by the whole-of-force and by Joint Task Forces. An NCW-capable force, or *Netforce,* is defined as a group of capabilities configured into a force that exhibits the desired NCW behaviour.

An individual project or capability would only be expected to exhibit NCW behaviour when it is deployed as part of a Netforce. However, individual projects and capabilities should be ready and able to be deployed as part of a Netforce. The NCW Compliance Process will initially check for this *Net-Readiness* of individual projects. The Net-Readiness concept is that projects that comply with endorsed Netforce Design principles and minimum Net-readiness standards could be readily combined into a Netforce without needing to develop new interfaces between interacting projects. This is contrasted with the more traditional system-centric approach in which customised one-to-one interfaces are developed to connect each pair of interacting projects. Note that for legacy projects, a wrapper may be required to enable interfacing to the network (Section 3.1).

3.5 Compliance not Assessment

The proposed NCW Compliance Process will check that projects comply with agreed minimum standards for Net-readiness.

Australia does not at present have a Technical Reference Model (TRM) that sets out the standards with which Defence Projects should comply. This is flagged as a critical issue for the NCWPO to resolve (Appendix A – Critical Issues List). The NCW Compliance Process is being developed as a learning model, so that it can be iteratively updated when additional standards guidance becomes available. In the interim, compliance is checked against the Defence Information Environment (DIE) Australian Technical Standards List (ATSL) [OCIO 2005]. The ATSL is a document that sets out the standards that are currently mandated by the Office of the Chief Information Officer (OCIO) for use by projects

[1] DSTO's Head, NCW Strategic Initiative (Dr Terry Moon) has recently established the Networked Joint Task Force (NJTF) 2015 Exploratory Study to address this issue.

intending to integrate with the DIE. The ATSL is to be used by all ADO staff, Defence consultants and contractors, responsible for DIE-related capability development, architecture development, procurement and projects.

The NCW Compliance Process does not presently assess the quality of projects or their contribution to overall NCW capability as part of a Netforce. In the future, the NCW Compliance Process will be expanded to include an NCW Assessment component that will assess the net-centric behaviour and performance of a project integrated into a Netforce. This Netforce Assessment component will link into the Defence Material Organisation (DMO) Test and Evaluation (T&E) processes and Defence Experimentation initiatives.

4. NCW Compliance Process Overview

4.1 NCW Compliance Components

The NCW Compliance Process includes NCW Compliance Components that span all three layers of the NCW enterprise model (Section 3.2). Figure 2 shows how the NCW Compliance Components align with the NCW enterprise model.

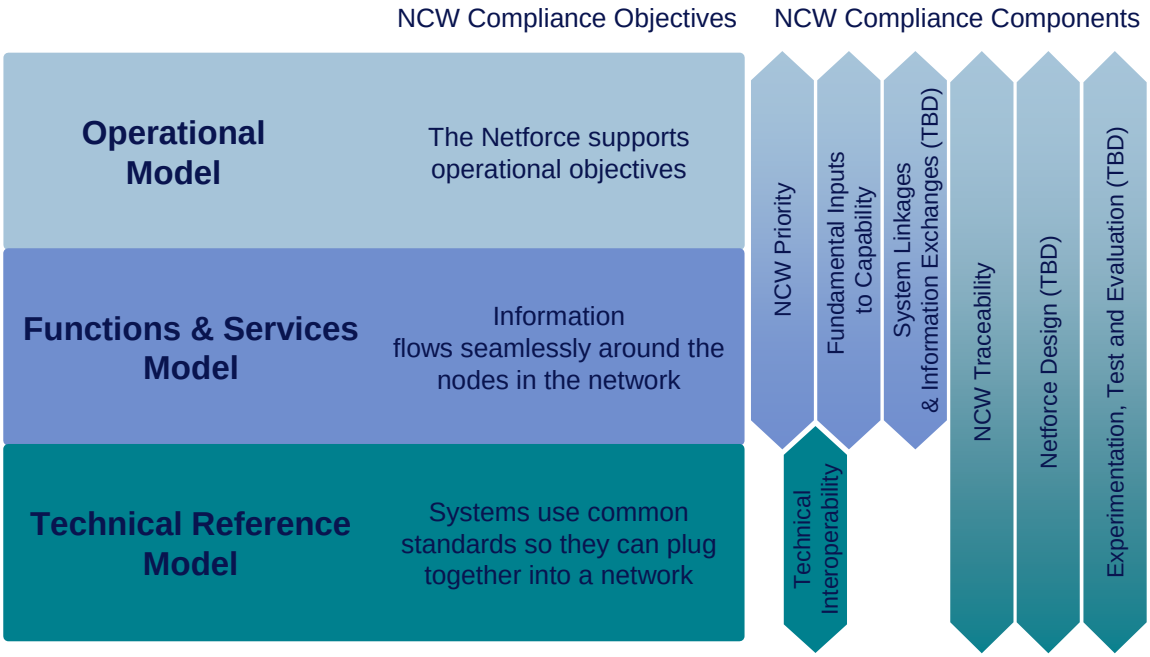


Figure 2 NCW Compliance Components

So far, four of the seven proposed NCW Compliance Components have been developed. These are the *NCW Priority*, *Fundamental Inputs to Capability* (FIC); *Traceability* and *Interoperability* components. These four components focus on checking projects for Net-readiness (eg checking for compliance with agreed standards). It is proposed to develop an additional three components, in follow-on work programs. These are the *System Linkages & Information Exchanges*; *Netforce Design* and *Experimentation, Test & Evaluation* components. These three components would focus on assessing the behaviour of projects or capabilities as part of a Netforce.

The NCW Compliance Components are summarised in Table 1. Appendices D to H provide additional details on the content and rationale for each component.

Table 1 NCW Compliance Components

Net-Readiness Components	
NCW Priority	Checks whether the project is (or should be) included in the NCW Roadmap and Integration Plan. This component is used as a filter, to identify projects that need to be checked for NCW compliance.
Fundamental Inputs to Capability (FIC)	Ensures that the project has identified and addressed the impact of NCW Compliance on FIC elements.
NCW Traceability	Ensures that the project's design and documentation support NCW guidance and provide a traceable path from NCW guidance to operational activities, system functions and services and then to the necessary technical standards.
Technical Interoperability	Ensures that the project complies with agreed technical standards for data, information and network interoperability.
Netforce Assessment Components	
System Linkages and Information Exchanges (to be developed)	Will be used to identify legacy and future systems that will need to exchange information with the project under assessment. This component could also be used to prioritise legacy systems for which a wrapper should be developed to enable interfacing to the Netforce.
Netforce Design Component (to be developed)	Will be used to ensure that projects are consistent with Netforce design attributes, e.g. architecturally and functionally consistent.
NCW Experimentation and T&E Component (to be developed)	Will be used to test and assess the delivered capability's behaviour in a Netforce environment.

Each NCW Compliance Component has three main parts:

1. A set of compliance questions, most of which have yes/no answers.
2. Exception handling of any variances, which involves the desk officer logging the exception and conducting an initial assessment of the expected impact of the variance. Action list items are flagged where additional support will be required from the NCWPO or other subject matter experts.
3. A reporting component, in which the desk officer ensures that compliance actions are recorded, required information is included in the project documentation, and certification is obtained from the NCWPO before the project proceeds to committee.

Appendix C lists the compliance questions for the four NCW Compliance components that have been developed to date.

4.2 Alignment with Defence Capability Development Process

The NCW Compliance Process aligns with the Defence Capability Development Process [DCOP 2006]. The NCW Compliance Process will be conducted at three stages:

1. First Pass
2. Second Pass
3. Acquisition.

As shown in Figure 3, each component may be applied at the First Pass, Second Pass or Acquisition stage of the Capability Development Process. For most of the components, the level of detail will tend to increase at later stages, reflecting the increase in detail and maturity of project documentation as the project progresses through the Capability Development Process. So far, the NCW Compliance process has focussed on Net-readiness checks that can be conducted at the First Pass and Second Pass stages. Further development is required before the NCW Compliance process can be applied at the Acquisition stage. This further development will require significant liaison with DMO.

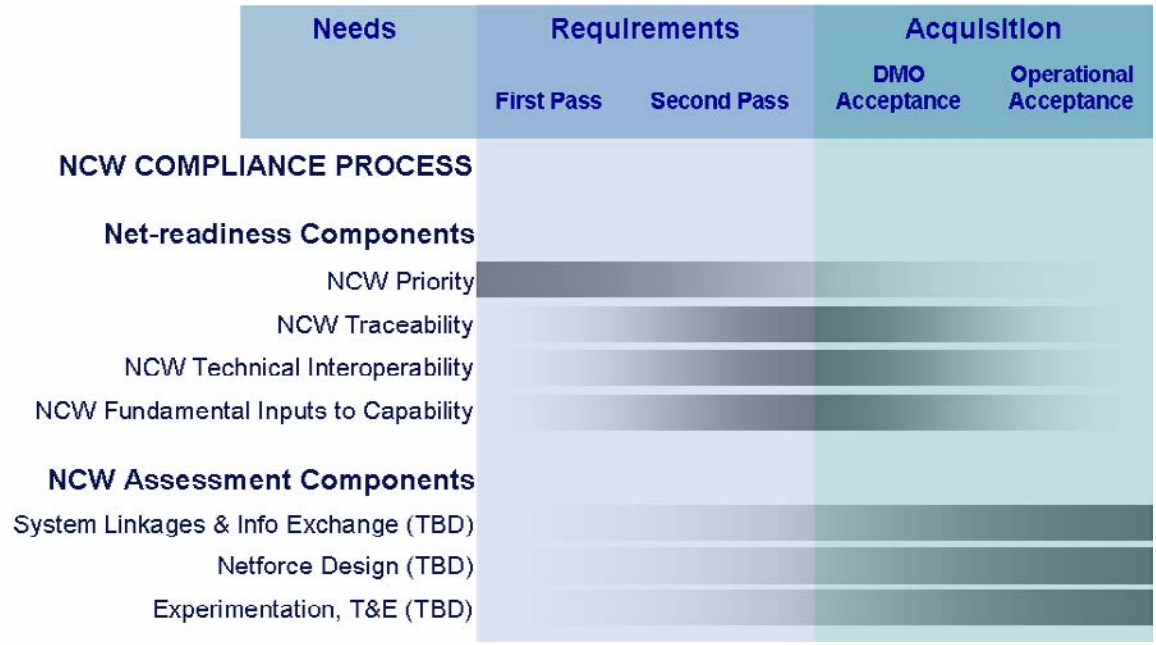


Figure 3 NCW Compliance Alignment with Capability Development Process

DNCWPO is responsible for certifying the project's NCW compliance status before the project documentation goes to committee for approval at the First Pass, Second Pass and Acquisition stages. The NCW Program Office will establish an NCW Support Team to provide desk officers with information about NCW compliance issues. The team will assist desk officers to adopt appropriate standards and develop project documentation that is consistent with NCW guidance. In the future, the NCW Support Team will assist DMO to test projects for compliance against defined NCW standards and stated NCW-related requirements. The NCW Support Team skill set is flagged as a critical issue for the NCWPO to resolve (Appendix A – Critical Issues List).

4.3 Process Model

Figure 4 provides a high-level overview of the NCW compliance process. The NCW Priority Component will be used as a filter to identify any projects that do not need to proceed to full NCW Compliance Assessment. This filter is intended to reduce the workload for desk officers and NCWPO staff by allowing them to focus on those projects that are expected to have a high impact on the ADO's future NCW capability.

For selected projects, Net-readiness checks will be conducted at the First Pass stage, based on the contents of the project's preliminary documentation. More detailed checks will be conducted prior to Second Pass, based on the project's more detailed documentation. In future, there will also be an NCW Assessment performed during the capability acquisition stage, prior to capability acceptance.

Appendix B provides a more detailed view of the NCW Compliance Process model, showing the flow of the compliance checks. This process model will need to be implemented in a user-friendly tool that assists the desk officers to complete the necessary checks, record the details and produce any required documentation.

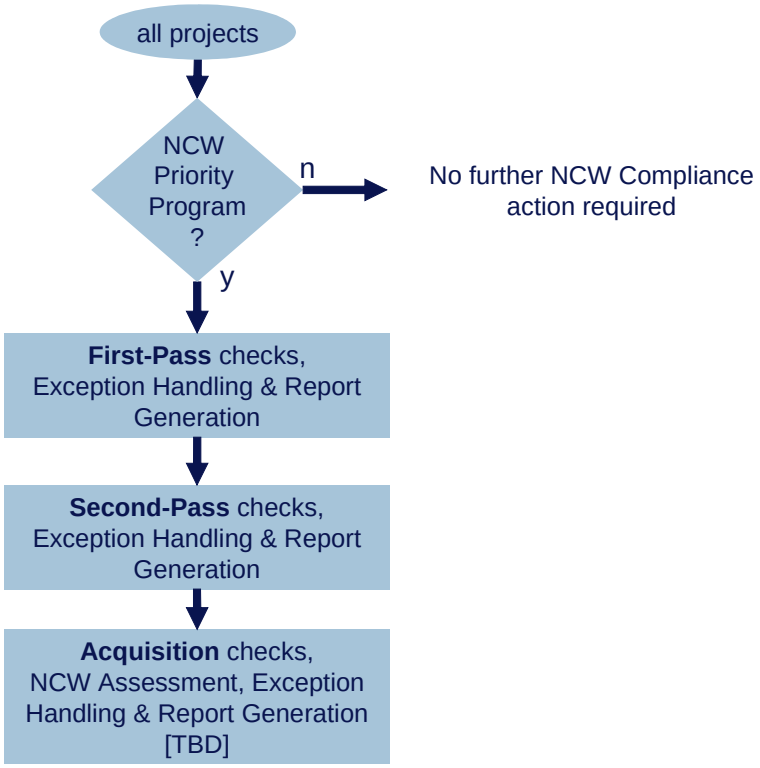


Figure 4 NCW Compliance Process Overview

5. Implementing the NCW Compliance Process

5.1 How DCP projects are handled

An NCW Compliance Process will be introduced in 2006. It will be applied to all projects within the Defence Capability Plan (DCP) that have not yet reached the acquisition stage (i.e. all projects at the Needs Stage, First Pass or Second Pass). The NCW Priority component may be used to reduce the workload on the NCWPO and desk officers, by identifying those projects that do not need to be fully checked for NCW compliance.

All projects in the NCW Roadmap and Integration Plan will be fully checked for NCW compliance. For other projects, as a general guide, if the project will be available after 2015, if it will deliver major systems that provide a significant C3I, sensing, effects or logistics capability and if it requires access to RT/NRT data then it should be checked for NCW Compliance and added to the NCW Roadmap and Integration Plan. For other projects (eg replenishment of stores) no further NCW Compliance action is required and the project can proceed through the normal Defence Capability Development Process.

5.2 Information Sources

The main information sources that will be used to undertake NCW Compliance checking will be the usual Defence Capability Development Process documentation (preliminary and final versions), including [DCOP 2006]:

- Operational Concept Documents (OCD) with associated Defence Architecture Framework (DAF) diagrams
- Function and Performance Specifications (FPS)
- Test Concept Documents (TCD)
- Requests for Proposal/Tender (RFP/RFT).

CDG mandates the form and content of the project documentation. CDG has mandated that all DCP projects must develop a set of DAF diagrams or *views*. These diagrams are expected to be particularly useful sources of information during the NCW Compliance process.

Where any of the DCP documents or the mandated architecture views are missing or incomplete, an additional workload will be imposed on the desk officer or NCWPO support team to produce the documentation, conduct compliance checks in the absence of the required documentation, or assess the risk of not completing the checks. This has been raised as a critical issue for the NCWPO to address (Appendix A).

In addition, the NCW Compliance process includes placeholders for an endorsed set of NCW Principles and a Defence Technical Reference Model (TRM). These have been raised as critical issues for the NCWPO to address (Appendix A). In the absence of a mandated TRM, the default is to use the ATSL as a key information source for standards checking.

5.3 Industry Implications

The NCW Compliance Process will impose some additional requirements on tenderers, but these are not expected to be onerous. In many cases, the NCW implications will initially be limited to requesting that the company provides a list of all the standards with which its offered solution complies.

In the future, Requests for Tender (RFT) and Requests for Proposal (RFP) might specify a list of Defence standards with which offers should comply. For example, the RFT/RFP's might require tenderers to be compliant with the project's standards profile (as shown in the project's DAF Technical views). Furthermore, where a prospective tenderer proposes any variances from such technical standards profiles, the tenderer should provide an assessment of the impact of the variance. Standards compliance should be enforced when a Technical Reference Model has been developed for the ADO.

In the future, RFTs might also include a requirement for the vendor to deliver a model that can be used by the ADO for test and evaluation (T&E), simulation and/or experimentation. Models might be used at the tender assessment or operational T&E stages of the acquisition process, or once the capability has entered service (e.g. for training or as a decision-aid).

5.4 Stakeholder Responsibilities

Desk Officers within Capability Development Group (CDG) are responsible for preparing project documentation in accordance with Defence policy and mandates. This project documentation will be the primary source of information for the NCW compliance process.

DNCWPO is responsible for certifying each project's NCW Compliance status, prior to Defence Capability Committee (DCC) meetings. The NCWPO Support Team is responsible for providing specialist NCW, systems and architecture support to assist the desk officer to complete the NCW Compliance checks. Appendix A includes a suggested skills profile for the NCWPO Support Team.

DMO's role in the NCW Compliance Process has not yet been established, but is likely to include responsibility for testing project performance in an NCW environment.

Industry is responsible for delivering a project that meets Defence requirements as specified in the tender documentation, including those requirements related to NCW.

5.5 Continuous Improvement of the NCW Compliance Process

It is recommended that the proposed NCW Compliance Process and checklists should be tested by running a candidate project through the NCW Compliance Assessment checklists and obtaining feedback from the desk officer and NCWPO support team.

Since technologies, international standards and NCW concepts will inevitably evolve over the next ten to fifteen years, it is critical to establish a means for the NCW Compliance Process to track and adapt to such changes. The NCW Compliance Process is being developed as a learning model, so that it can be iteratively updated and improved. It includes place-holders for compliance checks that will need to be introduced when a set of NCW Principles and a Technical Reference Model have been endorsed.

It is proposed to embed feedback loops within the NCW Compliance Process so that it is reviewed in response to:

- Changes to NCW guidance (e.g. release of an NCW Roadmap update)
- Changes to international standards and best practice in NCW
- Lessons-learned from ADF experimentation processes. Note that in addition to triggering a review of whether the NCW Compliance Process is delivering the desired ADF NCW capability, lessons-learned from experimentation might also trigger updates of higher-level guidance as Defence becomes aware of what is technically feasible and seeks to keep pace with international best practice
- Exception handling (for example, when a project seeks exemption from a mandated technical standard)
- Feedback from users of the NCW Compliance Process. The NCW Compliance Process Model and NCW Compliance Question List include questions designed to check that users are receiving appropriate support from each stage of the process and to elicit their suggestions for improvement.

Rather than reviewing the process every time a trigger event occurs, it is recommended that the NCW Compliance Process should be reviewed in line with updates to the Defence Capability Development Manual [DCOP 2006].

5.6 Further work

Further work is required to:

- Implement the proposed NCW Compliance Process Model. Issue 8 in Appendix A provides some suggestions and discussion of implementation issues.
- Develop the remaining components of the NCW Compliance Process, specifically the components associated with identifying key system linkages and information exchanges, ensuring a consistent NCW functional design, and assessing each project's performance in a Netforce environment by means of experimentation (including modelling and simulation) and test and evaluation. Appendix H provides an outline of the additional compliance components that should be considered.

6. Outcomes of the Compliance Process

6.1 Delivering the Netforce

The NCW Compliance Process is about more than checking for Networking capability (i.e. communications connectivity). NCW will impact across most of the FIC elements. At the initial Net-readiness stage, the focus is on identifying priority projects, implementing common standards and ensuring that project documentation demonstrates a traceable commitment to supporting endorsed NCW guidance. Other NCW Assessment components would then test and assess each project's capability to operate in a Netforce environment.

6.2 Moving from Network-centric to Information-centric Warfare

The flow of information is central to the future Netforce. The network is relevant to the extent that it supports the flow of information. Therefore, the focus of the proposed NCW Compliance process is less on network connectivity and more on data compatibility. This has been described as an information-centric approach [Jacoby 2006] where:

- A wider range of information will be made available more quickly to a wider range of decision-makers and
- Decision-makers will be able to access the information they need, processed and presented in useful ways.

In the future Netforce environment, data will be tagged so that (for example) discovery tools can readily locate it and correlation tools can precisely manipulate it. Decision-makers will have access to information that gives the pedigree of the data (e.g. how and when it was collected). Groups of decision-makers will be able to more easily coordinate their decisions. Collection systems will have access to information that gives details on how the collected data will be used, so that more timely and appropriate collection processes can be planned. And data will be linked from sensor to decision-maker and sensor-to-shooter in shorter timeframes, to support increased speed and span of command. The NCW Compliance Process will support this future environment.

6.3 Other benefits of the NCW Compliance Process

The NCW Compliance process provides an opportunity to collate information about the characteristics of DCP projects in a standardised format. This information could be stored in a central repository (e.g. TARDIS) for discovery and access by a wide range of authorised Defence users. The information could be used to simplify future NCW Compliance Assessments by re-using relevant material. It might also be useful for planning deployments and experimentation programs, by providing information about the capability of defence projects to operate in a Netforce environment.

The NCW Compliance Process also provides an opportunity to ensure compliance with mandated documentation and DAF requirements (where these products are relevant to assessing Net-readiness and delivering capability).

7. Summary

This document provides an overview of a proposed NCW Compliance Process, a detailed Process Model (Appendix B) and Compliance Question List (Appendix C) that could be implemented by the NCWPO.

It also identifies (Appendix A) the following critical issues to be addressed by the NCWPO in order to improve the rigour and quality of the NCW Compliance Process:

1. Systems and Operations Analysis effort to translate the ADO's NCW guidance for the whole-of-force into Netforce principles and target states that can be checked for individual projects
2. Development of an Australian Netforce Design and supporting Technical Reference Model
3. An assessment of the case for Services-Oriented Architectures for the ADO
4. Development of an architecture schema for the current and future ADO
5. Compliance with CDG mandates for Capability Project Documentation
6. Establishment of an NCWPO Support Team with an appropriate skills profile.

The NCW Compliance Process should be updated as these issues are addressed, and in response to feedback from the NCWPO Support Team and desk officers who use the process. It is recommended that the NCW Compliance Process should be reviewed in line with updates to the Defence Capability Development Manual .

This report delivers the Net-readiness components of the NCW Compliance Process. It is recommended that additional work should be undertaken to develop the Assessment components of the NCW Compliance Process, which will focus on assessing the capability of Net-ready projects to operate in a Netforce environment.

8. References

ADFP 20 (1999) "Logistics In Support Of Joint Operations" Commandant, Australian Defence Force Warfare Centre, Defence Publishing Service, Department of Defence, Canberra ACT

Alberts, DS (2002) "Information Age Transformation", CCRP, United States, ISBN: 1 893723-06-2.

Alberts, DS, Garstka, JJ & Stein, FP (1999) "Network Centric Warfare", 2nd Edn, CCRP, United States, ISBN: 1 57906-019-6.

Boyd, C., Williams, W. Skinner, D. and Wilson, S., (2005) "A Comparison of Approaches to Assessing Network-Centric Warfare (NCW) Concept Implementation", Proceedings of the

Systems Engineering , Test & Evaluation Conference, SETE 2005 – A Decade of Growth and Beyond, Brisbane, Queensland, 7 to 9 November 2005

C4ISR Architecture Working Group (1998) "Levels of Information Systems Interoperability (LISI)" US DoD, March 1998

Capability Development Group (CDG) (2005), "NCW Roadmap", Department of Defence, Canberra ACT, DPS: October/2005

DEFWEB (2006), "Fundamental Inputs to Capability", URL: http://defweb.cbr.defence.gov.au/strategypb/References%20and%20Documentation/Fundamental%20Inputs%20to%20Capability/Fundamental%20Inputs%20to%20Capability.doc

Director, Capability Options and Plans (DCOP) (2006), *Defence Capability Development Manual 2006*, Capability Systems Division, Defence Publishing Service, Department of Defence Canberra ACT

Dstl (2004) "The NEC concept", *Distillation*, 3rd themed issue: Network Enabled Capability, UK MoD

Jacoby, LE (2006) "Info-centric operations: Intelligence collection, handling and analysis undergo fundamental change", *C4ISR Journal*, Vol 5 No 1 January/February 2006 pp14-15 URL: http://www.isrjournal.com/story.php?F=1229768

Keus, HE (2005) "NETFORCE PRINCIPLES: An Elementary Foundation of NEC and NCO", 10th CCRT Symposium, June 13-16, McLean, Virginia, US

Kingston G, Richer W and Kohn E (2006), "NCW Risk Assessment Theory" 11th International Command and Control Research and Technology Symposium (ICCRTS), Australia, draft paper in preparation

McKenna, T, Moon, T, Davis, R & Warne, L (2006) "Science and Technology for Australian Network-Centric Warfare: Function, Form and Fit", *Australian Defence Force Journal*, Vol. 170

Ministry of Defence (MoD) (2005) "Network Enabled Capability", 01/05 C100, UK

NATO (2006) "C3 Technical Architecture Version 6" URL: http://nc3ta.nc3a.nato.int/

Office of the Chief Information Officer (OCIO) (2005) "Defence Information Environment (DIE) Approved Technology Standards List (ATSL)" Version 2.4, 19 Dec 2005 Australia

Polk, RB (2000) "A Critique of the Boyd Theory – Is it Relevant to the Army?" *Defense Analysis*, Vol. 16, No. 3, December, pp. 257-276

Richer, W, Kohn E, Kingston G (2006) "NCW Risk Assessment – Towards a Compliance Policy and Process", 11th International Command and Control Research and Technology Symposium (ICCRTS), Australia, draft paper in preparation

Tolk, Andreas (2003) "Beyond Technical Interoperability – Introducing a Reference Model for Measures of Merit for Coalition Interoperability", 8th International Command and Control Research and Technology Symposium, Washington DC

US Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer (US CIO) (2004) "Net-Centric Checklist" May 12, 2004 Version 2.1.3, URL: http://www.defenselink.mil/nii/org/cio/doc/NetCentric_Checklist_v2-1-3_May12.doc

US Department of Defense (US DoD) (2006) "Features of Net-Centricity", URL: http://akss.dau.mil/dag/Guidebook/IG_c7.2.6.1.asp

Appendix A: Critical Issues List

A.1. Systems and Operations Analysis

A systems and operations analysis process is required to translate the ADO's NCW guidance for the whole-of-force into Netforce principles and target states that can be checked at the individual project level. This analysis process would also provide the principles and guidance for an Australian Netforce Design (next section). DSTO's Head, NCW Strategic Initiative (Dr Terry Moon) has recently established the Networked Joint Task Force (NJTF) 2015 Exploratory Study to address this issue.

By checking projects against these Netforce Principles, the NCW Compliance Process would provide traceability from high-level guidance through to delivered capability. It would help to deliver a future force that can implement the ADO's aspirational warfighting capability.

A.2. Australian Netforce Design

It is not currently possible to check that projects will support the ADO's NCW aspirations when configured as part of a Netforce. This is due to the lack of a rigorously defined system-of-systems model for the Netforce. On a fundamental level the science and engineering of networks is in its infancy. However, researchers have begun to develop modelling frameworks of elementary principles from which NCW concepts can be constructed and derived [Keus 2005].

A Netforce system-of-systems model or *Netforce Design* would identify the architecture schema, characteristics and functional design attributes of a future Australian Netforce. It would include a generic NCW functions and services model (probably based around the commander's sense-decide-act cycle [Polk 2000]). An Australian Netforce Design would also provide a basis for expanding the NCW Compliance Process to include an Experimentation, Test and Evaluation (T&E) component. This component would provide a means of checking that an individual project or capability is capable of being integrated into a Netforce and exhibits desired NCW behaviour when it is deployed as part of a Netforce.

A.3. Technical Reference Model (TRM)

The purpose of a Netforce TRM is to provide a common conceptual schema and a common vocabulary for guiding the integration of legacy and future capability projects into a Netforce, with the aim of improving interoperability, portability, scalability and cost-effectiveness of procurements. Technical interoperability is dependent on the establishment of a common set of services and interfaces that system developers can use to resolve integration issues associated with the technical architecture of legacy and proposed capabilities. The TRM structure is intended to reflect the separation of data from applications and applications from the computing platform — a key principle in achieving open systems.

This approach of using a TRM provides a standards-based method for assessing technical interoperability. The TRM provides the framework for a set of agreed standards both current and emerging and the reference for all components that need to interface with the Netforce in a manner that is both consistent and managed.

Australia does not at present have an endorsed Technical Reference Model (TRM) that sets out the standards with which Defence Projects should comply. The Australian Technical Standards List (ATSL) is a list of standards categories, but not a technical reference model. The ATSL references the US DoD JTA TRM [OCIO 2005], but the US has migrated from the JTA to a new model called the Net Centric Operations and Warfare (NCOW) Reference Model [US DoD 2006] as a part of their transition towards NCW. The Australian Defence Organisation (ADO) has chosen, at this point in time, not to link to the US NCOW TRM.

There should be consistency between the ATSL, the Defence Tactical Information Exchange (TIE) standards and with any future Australian TRM. For example, an endorsed TRM for an Australian Netforce could integrate all relevant standards for ADO systems. Congruence with US, NATO and other coalition partner standards should be considered.

Furthermore, Defence should decide on the type of technical reference model it wishes to adopt. For example, the US and NATO have adopted services-oriented TRMs. Defence should also decide what type of TRM (i.e. technical infrastructure architecture) it wishes to adopt. This issue is particularly relevant to the Netforce development and is discussed further in the section on Services-Oriented Architectures.

By checking projects against the TRM, the NCW Compliance Process will establish greater consistency between projects, thereby leading to improved interoperability between Australian and (potentially) coalition systems. The NCWPO should consider whether capability projects should develop a standards profile based on the TRM and whether this standards profile should be included in RFT/RFPs. Doing this would enable the NCWPO (and DMO) to check that offered (and delivered) capabilities comply with agreed Defence standards.

A.4. Services-Oriented Architectures

The US government, NATO and commercial IT organisations are moving to implement services-oriented architectures (SOA) where appropriate, but the ADO appears to be reluctant to initiate such a move. This reluctance is despite the ADO placing a high priority on interoperability with the US and stating a desire to, where possible, leverage off commercially-available technology. This could ultimately affect the level of interoperability that can be achieved in coalition operations. The ADO should therefore investigate SOA in more detail and develop a strategy to ensure sufficient levels of interoperability can be achieved in net-centric coalition operations. It should be noted however that it may be difficult to retain high levels of interoperability in cases where the connecting architectures are conceptually different (eg system-centric versus net-centric).

Significant operational analysis and systems analysis effort may be required to assess whether Australia should adopt SOA. It would also be important to identify those

operational activities that suit an SOA approach. For example, SOA approaches are considered appropriate for exchanging (short) messages where some transmission delays are acceptable, i.e. where some transactional latency can be tolerated. The US Defense Force is using SOA in information exchange environments, for data gathering, discovery, exploitation, picture formation and dissemination. However, SOA might not be appropriate in environments where safety-critical and time-critical responses are required. For example, tightly-coupled architectures might be more appropriate for fire control systems, countermeasures and mission safety critical systems. This raises the issue of tightly-coupled versus loosely-coupled architecture designs, and the appropriate operational scenarios for each.

If the ADO chooses to adopt a services-oriented approach, then it will need to identify the SOA characteristics and design principles that are relevant for an Australian Netforce. A services-oriented TRM would need to be considered (or a link to an existing SOA TRM, such as the US NCOW Reference Model). Even if an SOA approach is not selected, the ADO will need to agree on preferred styles of architecture for future Defence systems and include sufficient flexibility to be able to work effectively in coalition operations. Noting the dichotomy between tightly- and loosely-coupled architectures, the possibility of developing hybrid architectures should be investigated.

A.5. Whole-of-force Architecture Schema

A whole-of-force architecture schema for the current and future ADO is required so that new projects can readily identify key capability linkages. This would include a set of Defence Architecture Framework (DAF) products that represent the force at the operational, systems and technical levels (with associated link to a TRM). For example, a 2015 baseline architecture might include the OV-2, OV-3, SV-1 and TV-1 (and perhaps the TV-2) DAF products. Such a model would enable the NCW Compliance Process to check that proposed capabilities can interface to key ADO systems.

There is a need for consistency and interoperability across the DAF representation of the whole-of-force. The NCWPO might suggest that the Office of the Chief Information Officer (OCIO) develops and maintains a linked set of architecture products (system models) for each ADO capability – both legacy and proposed – within a consolidated data model. This would require that DAF products are produced in a consistent manner, in accordance with OCIO mandates. This might require, for example, the establishment of a methodology comprising an agreed set of methods, approved Computer Aided Software Engineering (CASE) tools, a common data model and global set of reusable data entities as well as the provision of a DAF guidebook and the development of a common dictionary or ontology.

Access to a consistent and interoperable DAF representation of the whole-of-force would provide a baseline for Netforce architecture development and would allow for the following types of analysis:

- Investigation of interactions with a new capability
- Impact of decommissioning an existing capability
- Baseline for modelling and simulation of system (and Netforce) behaviour.

A.6. CDG Mandates for Project Documentation

Defence Capability Development Group (CDG) mandates the form and content of Operational Concept Documents, Functional and Performance Specifications and Test Concept Documents. CDG mandates that DAF products will be developed.

Where projects do not comply with CGD directives and critical documentation is missing (such as TV-1 and TV-2 DAF products), the NCWPO will not be able to complete the NCW Compliance checks. Fallback options for the NCWPO would involve significant resources to develop the missing documentation, or perform a detailed assessment of the capability project (instead of a simple compliance check) or conduct a risk analysis of the impact of not having undertaken NCW compliance checking for the project. The NCWPO might recommend that CDG develops (or updates) a capability development guide and checklist to increase desk officer compliance with CDG mandates.

A.7. NCW Support Team Skills Profile

The NCW Compliance Process is being developed as an enabler. It provides desk officers with information about NCW compliance issues and assists them to adopt appropriate standards and incorporate appropriate material into their project documentation. In the future, it will incorporate an Experimentation, T&E component, to enable DMO to test projects for compliance with defined NCW standards.

The NCWPO's NCW Support Team will provide specialist NCW advice to desk officers and DMO, and assist them to conduct the NCW compliance checks. Therefore, the NCWPO requires a pool of appropriately skilled and experienced advisers that should include the following specific skill profile:

- Systems engineering across a range of methodologies and social models
- Capability engineering
- Enterprise architecting
- Systems analysis.

A.8. Implementation of the NCW Compliance Process

The current work program delivers an NCW Compliance Process Model that can be implemented in whichever format the NCWPO prefers. The following options have been identified for implementing the NCW Compliance Process:

- A requirements management tool such as Boreland's CORE ®
- Web-based front-end linked to a database
- Paper-based
- A combination of these.

It is recommended that the implementation of the NCW Compliance Process should:

- Include an easy-to-use interface that guides the desk officer through the compliance process

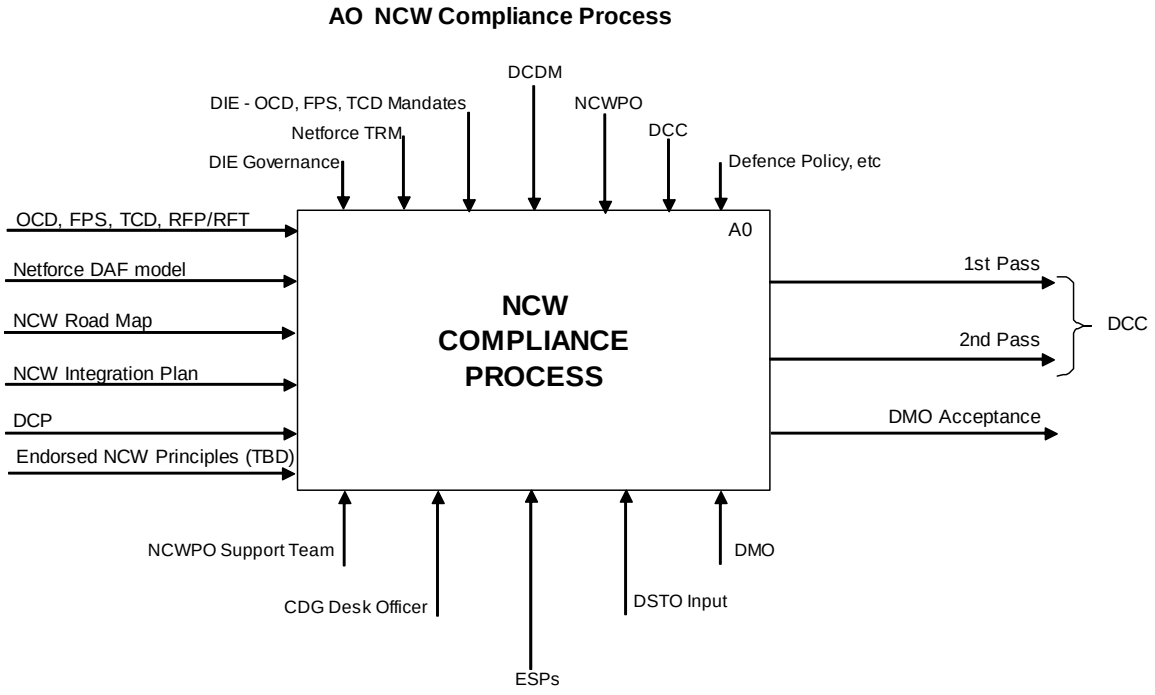
- Electronically record the results of the compliance checks, exception handling and NCWPO certification
- Collate all compliance data in a common database to for future reference/reuse
- Automatically generate any compliance reports required by the NCWPO or Defence capability committees
- Maintain a permanent record of compliance information that can be easily searched
- Be easily updated in response to new higher-level guidance, evolution of the compliance process and in response to user feedback.

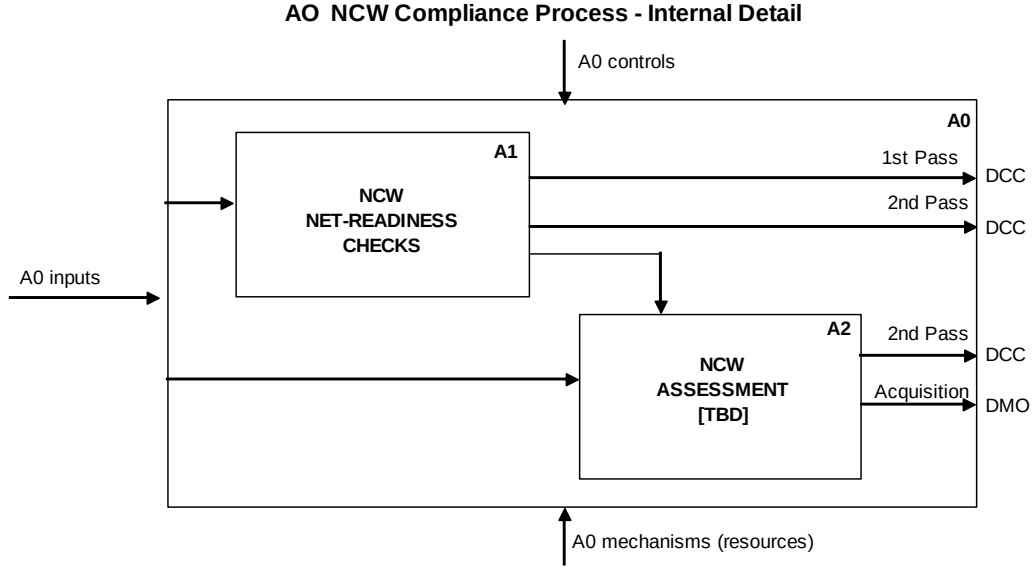
IMPORTANT NOTE: Although CORE would be a useful tool for documenting and planning the compliance process implementation, a web/database system is more likely to meet the above requirements for implementing the final product.

Appendix B: NCW Compliance Process Model

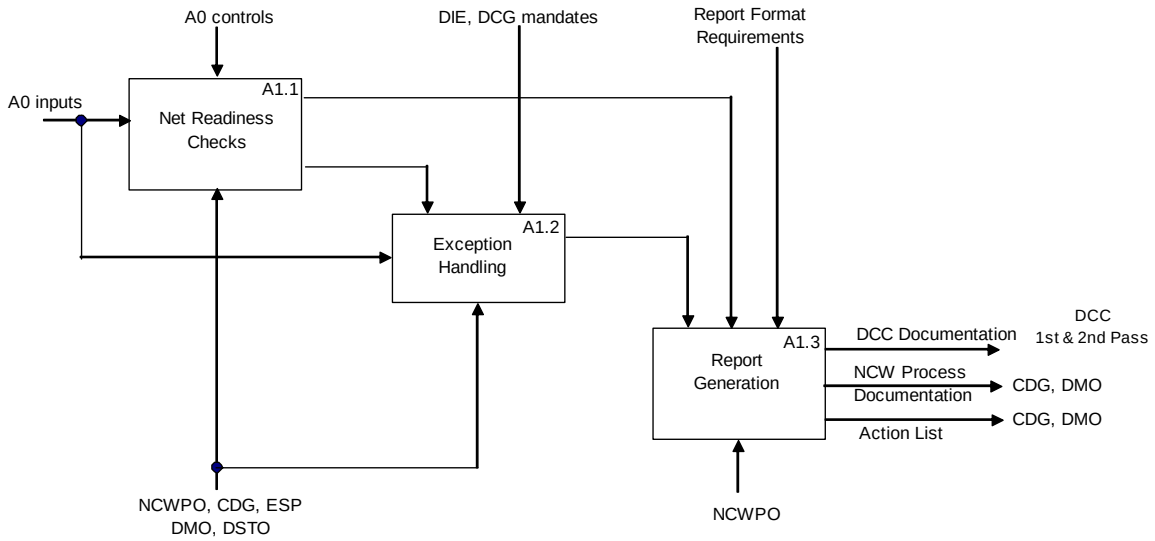
The following block diagrams summarise the inputs, outputs and actions that should be taken at each stage of the NCW Compliance Process. This material is intended to provide guidance to the NCWPO in implementing the proposed NCW Compliance Process.

B.1. High-level process overview

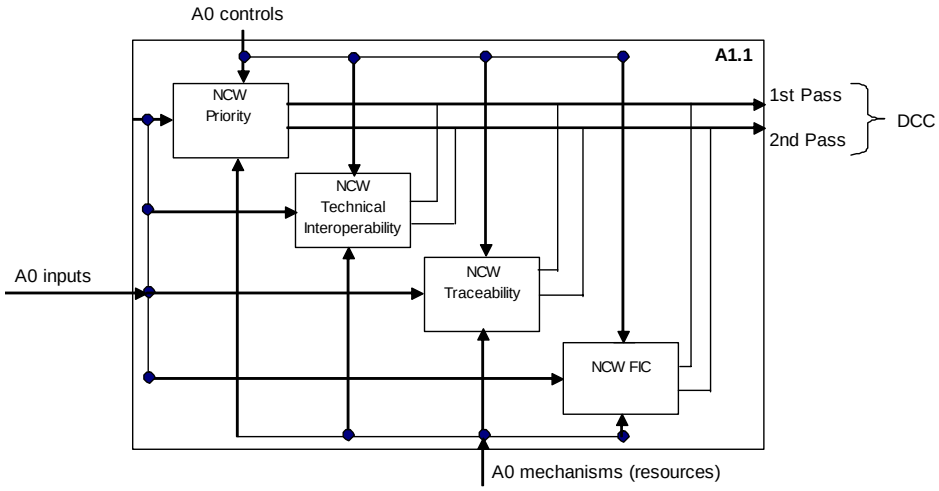




A1 Net Readiness Compliance Process

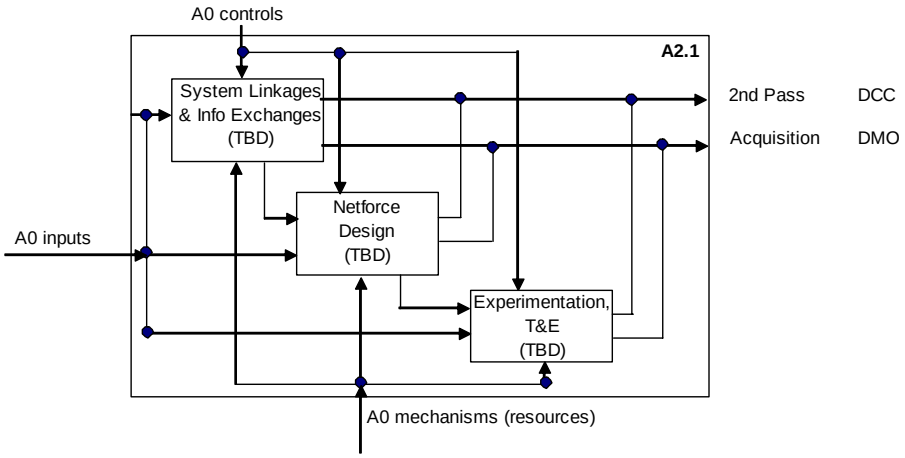


A1.1 Net Readiness Components

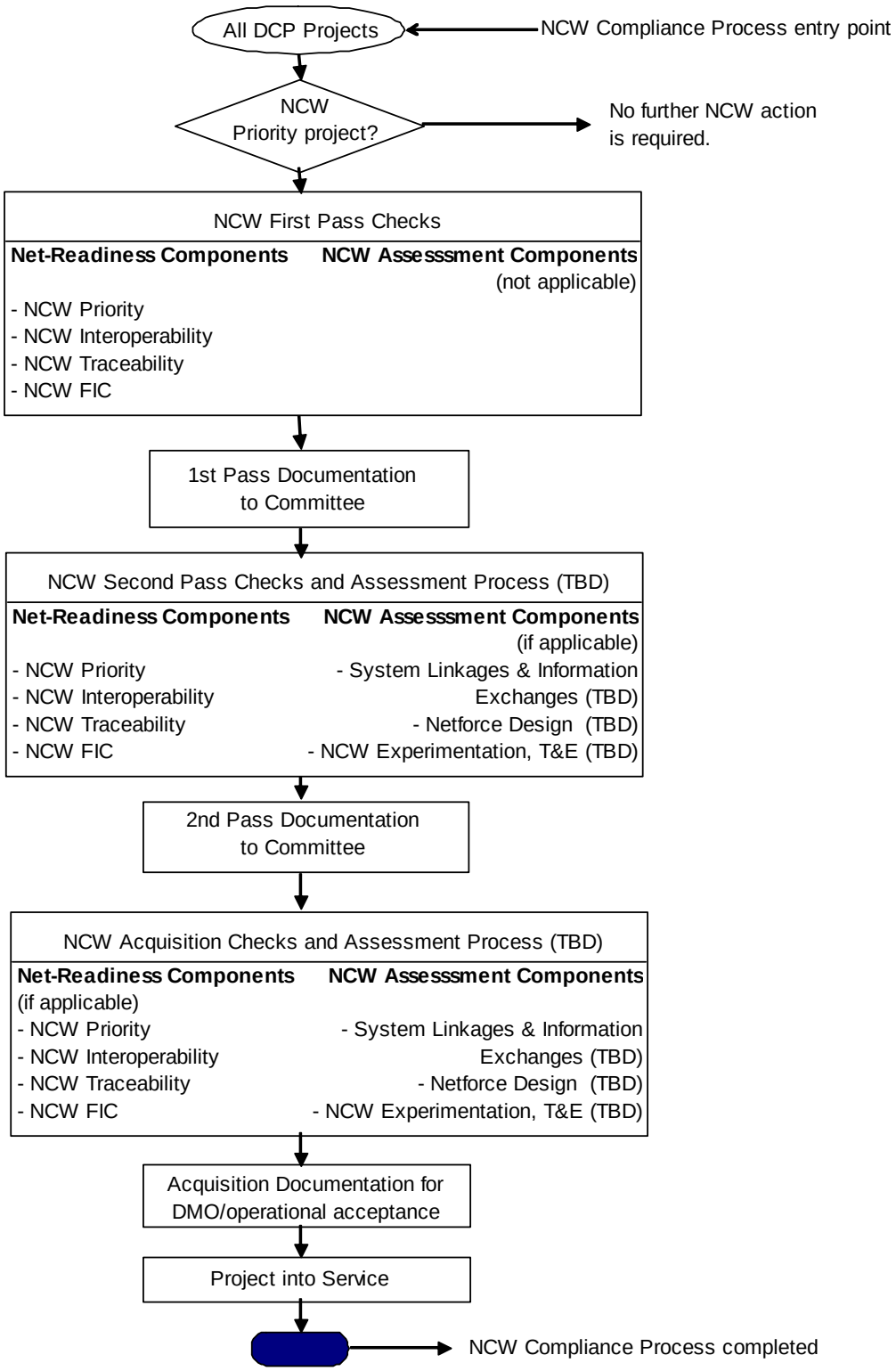


A2.1 NCW ASSESSMENT - TBD

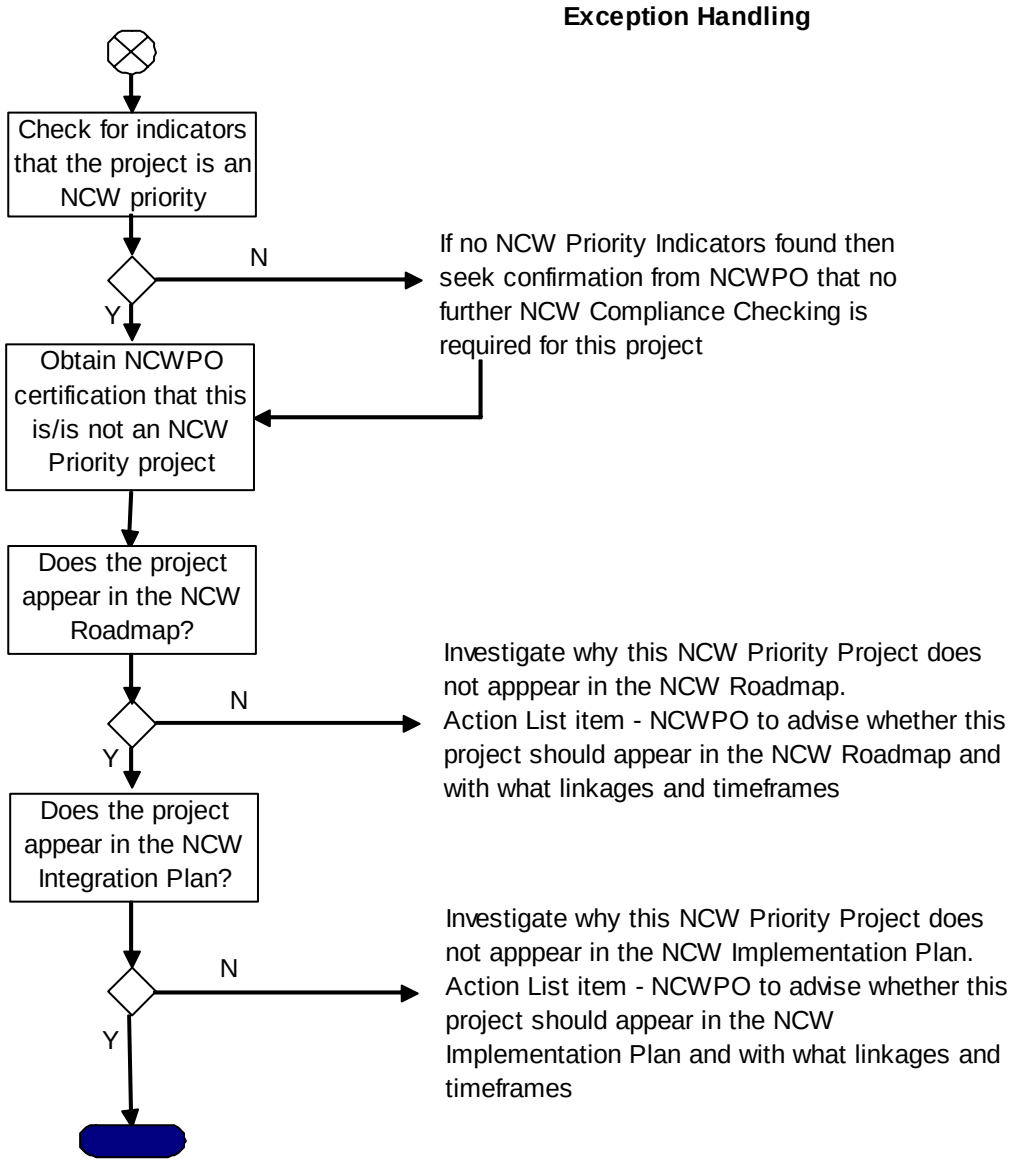
It is anticipated that the Assessment stage will include the following checks



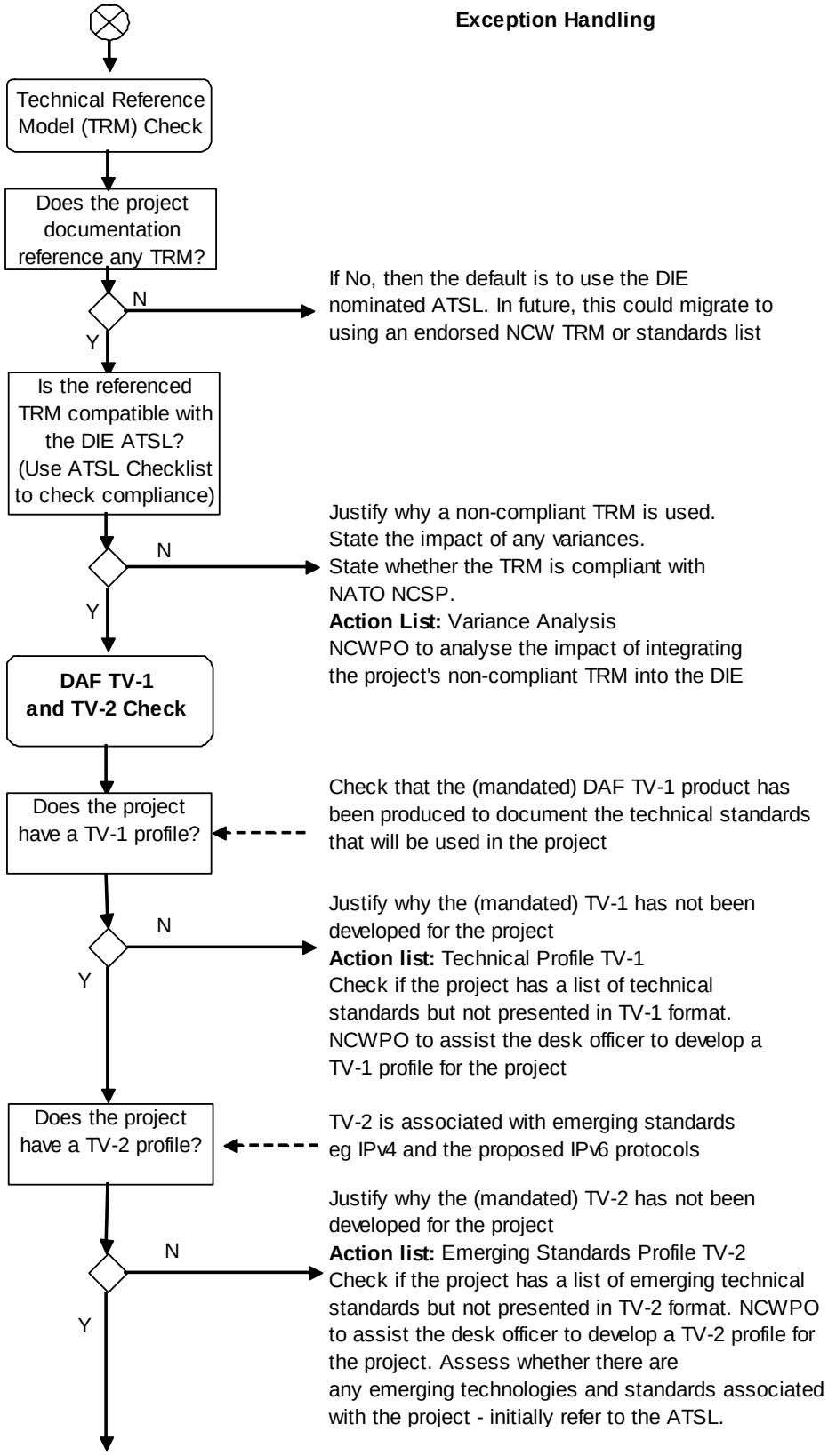
B.2. Master Process flow

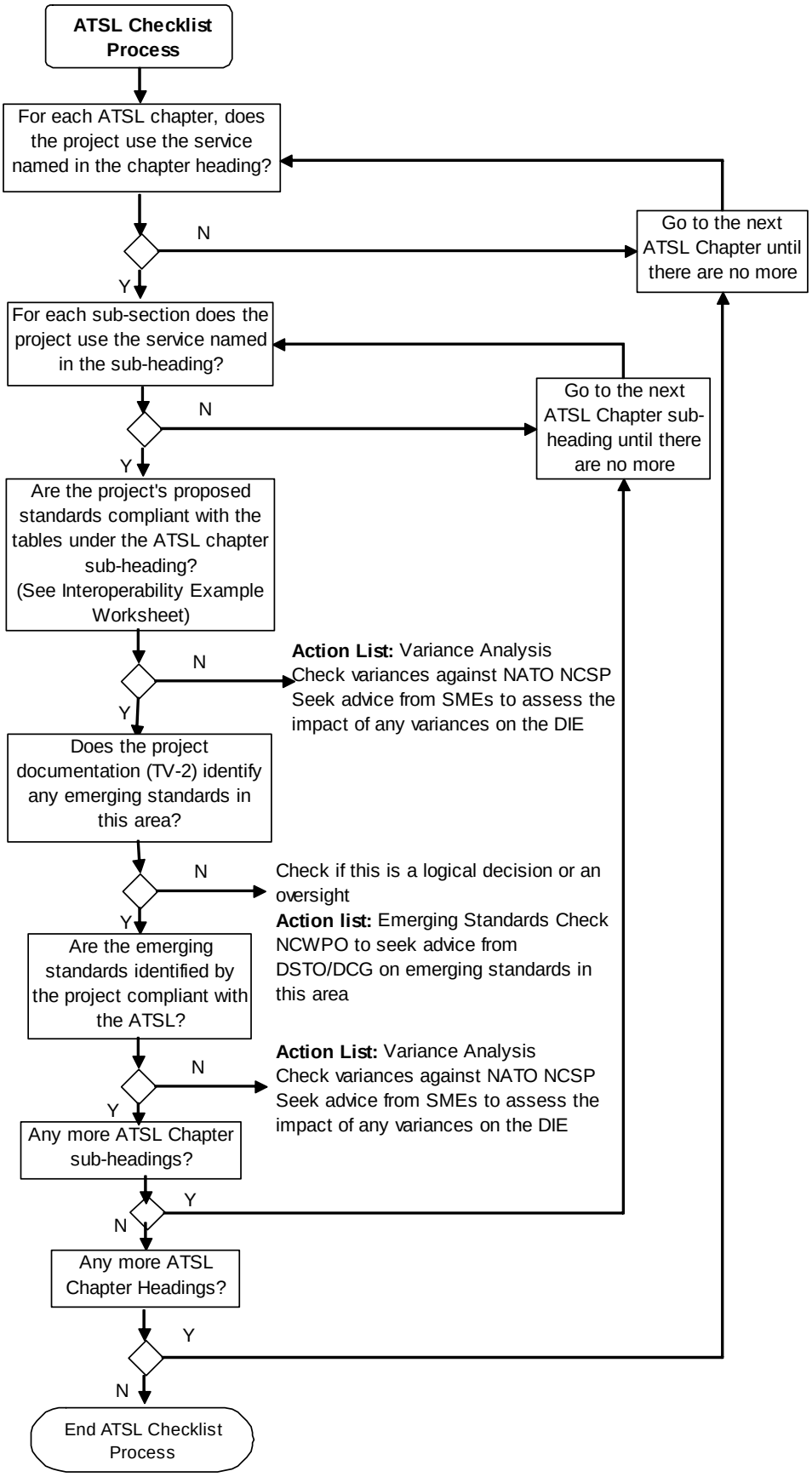


B.3. Priority Component

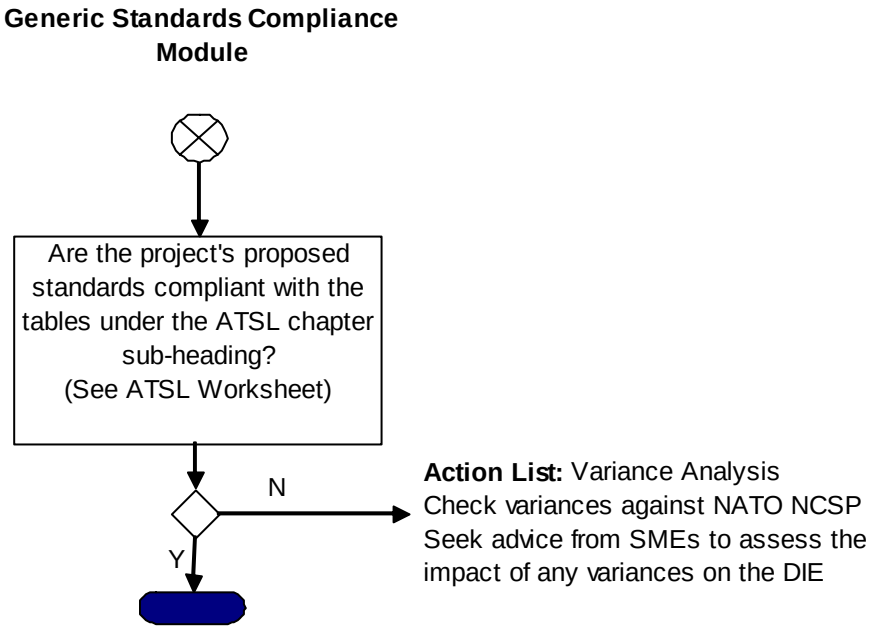


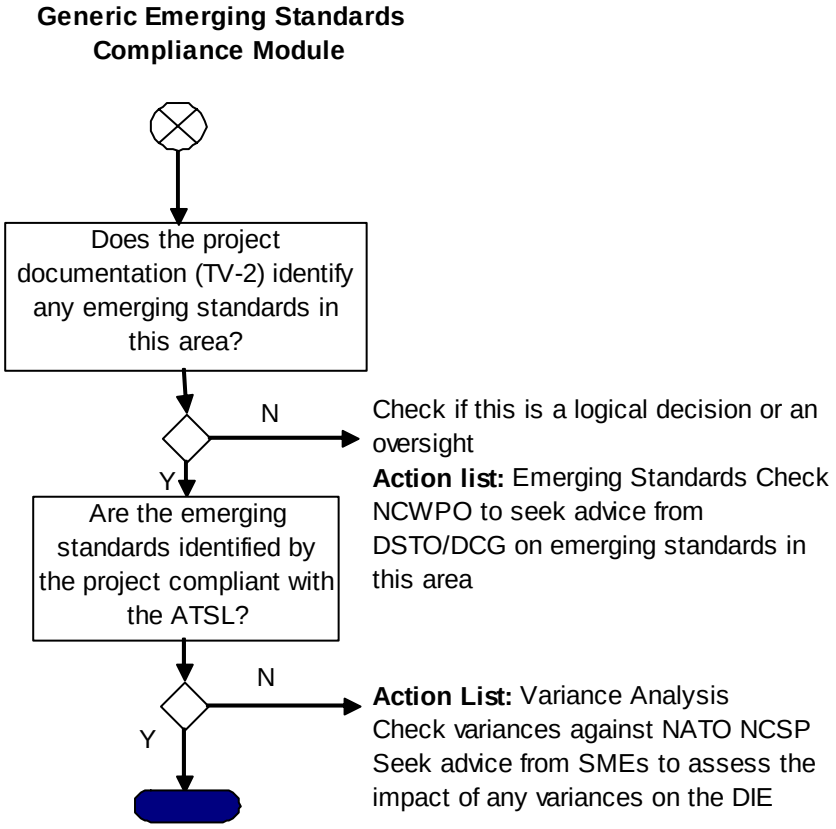
B.4. Technical Interoperability Component



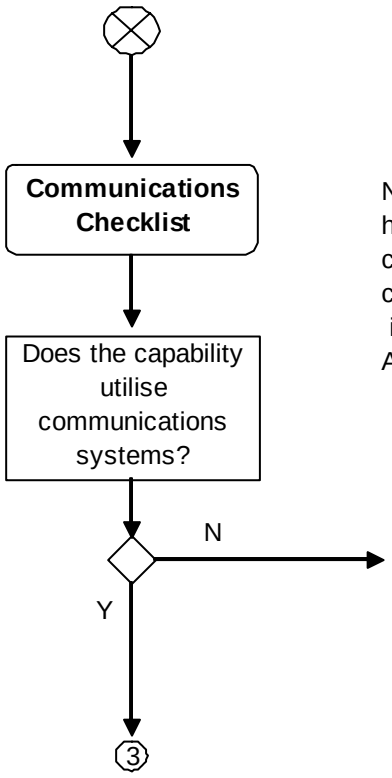

ATSL Checklist Process
For each ATSL chapter, does the project use the service named in the chapter heading?
N
Y
Go to the next ATSL Chapter until there are no more
For each sub-section does the project use the service named in the sub-heading?
N
Y
Go to the next ATSL Chapter sub-heading until there are no more
Are the project's proposed standards compliant with the tables under the ATSL chapter sub-heading? (See Interoperability Example Worksheet)
N
Y
Action List: Variance Analysis
Check variances against NATO NCSP
Seek advice from SMEs to assess the impact of any variances on the DIE
Does the project documentation (TV-2) identify any emerging standards in this area?
N
Y
Check if this is a logical decision or an oversight
Action list: Emerging Standards Check NCWPO to seek advice from DSTO/DCG on emerging standards in this area
Are the emerging standards identified by the project compliant with the ATSL?
N
Y
Action List: Variance Analysis
Check variances against NATO NCSP
Seek advice from SMEs to assess the impact of any variances on the DIE
Any more ATSL Chapter sub-headings?
Y
N
Any more ATSL Chapter Headings?
Y
N
End ATSL Checklist Process

B.5. Generic Standards Compliance Module





B.6. Interoperability Example – Communications

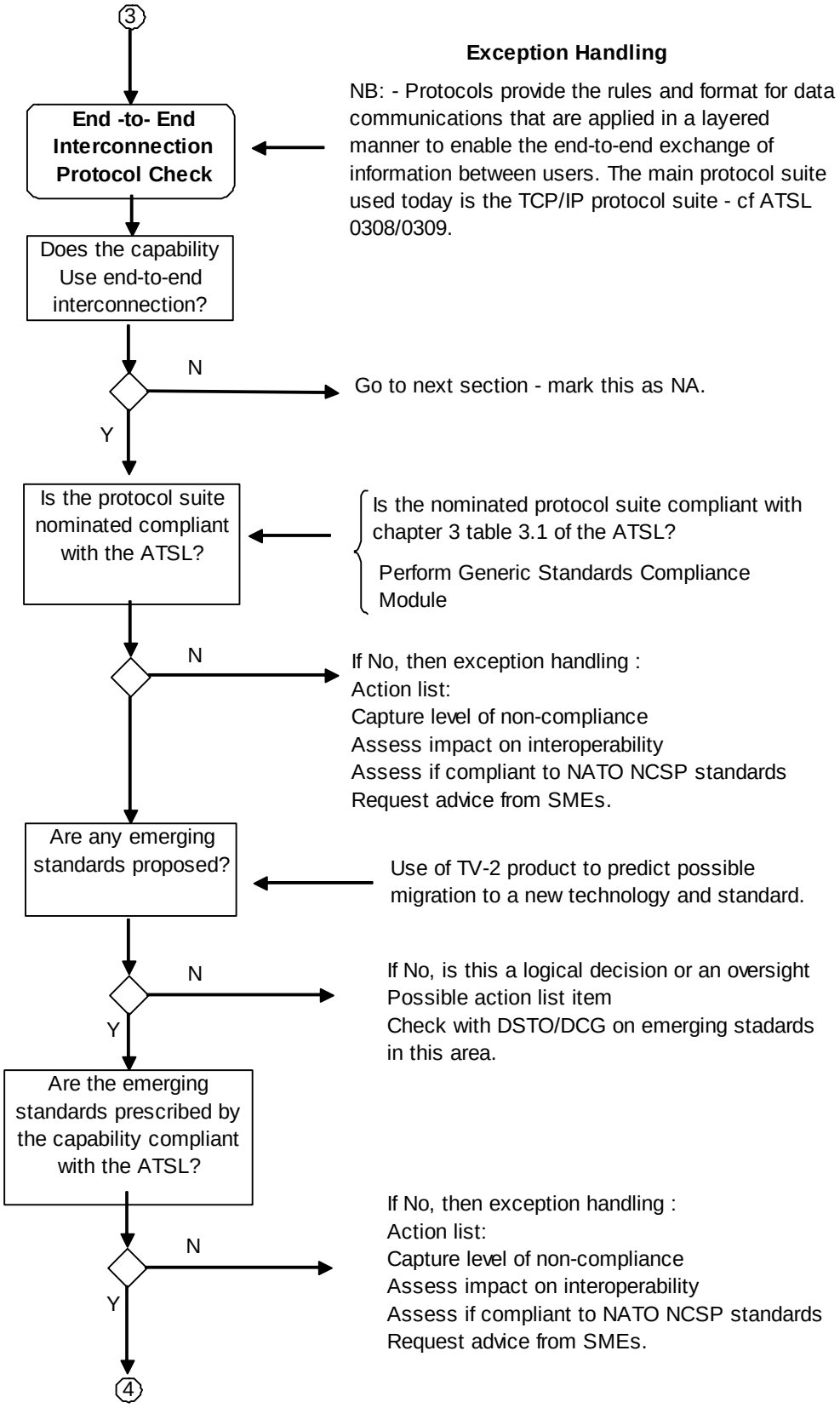


Exception Handling

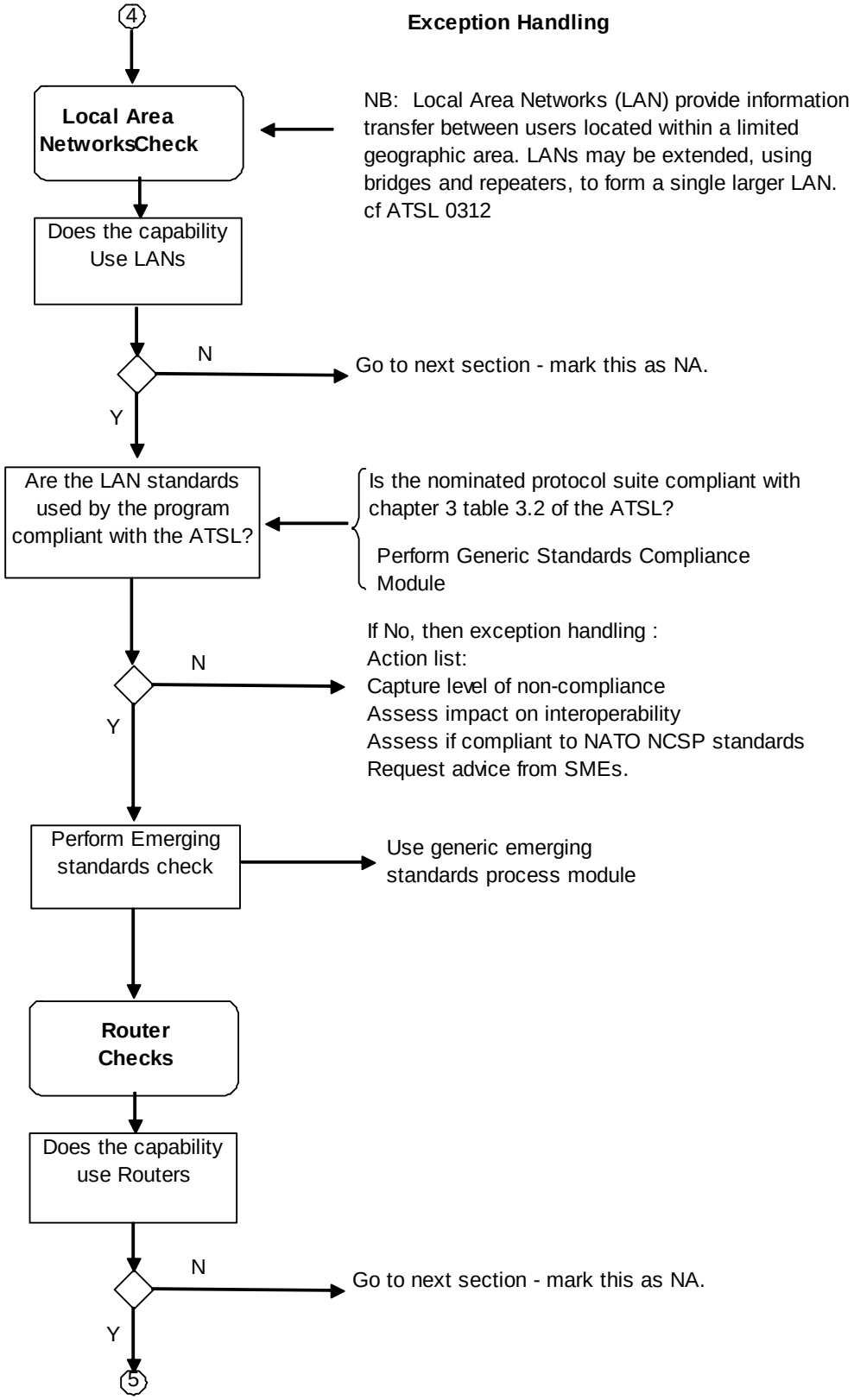
NB: Figure 3.1 from the ATSL - schematic of how communication components may be combined to specify communication networks capable of supporting voice and data. information transfer.
ATSL treats them at and below layer 4

If No then move to next category - Network Services Checklist

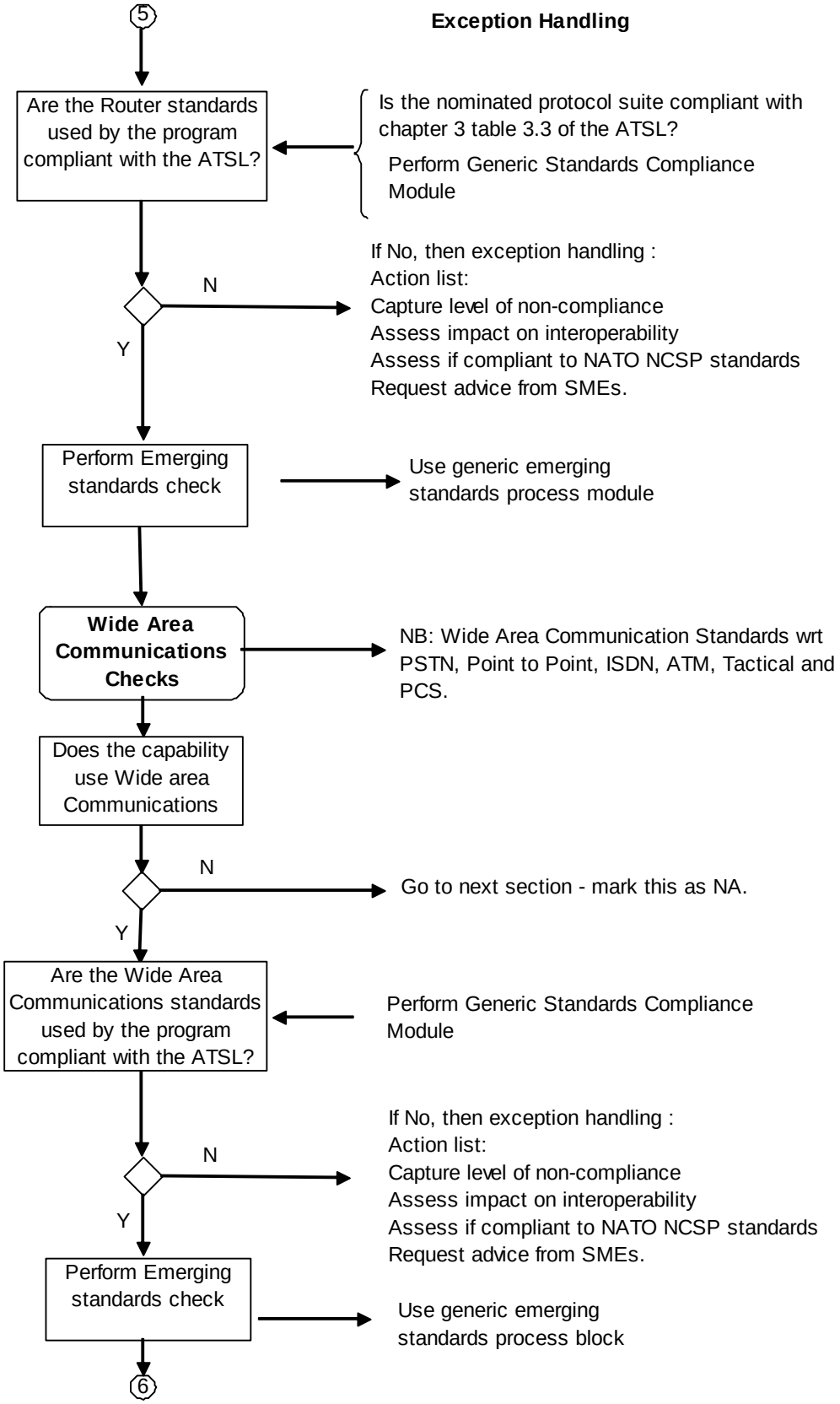
Net Readiness Example - Communications cont...



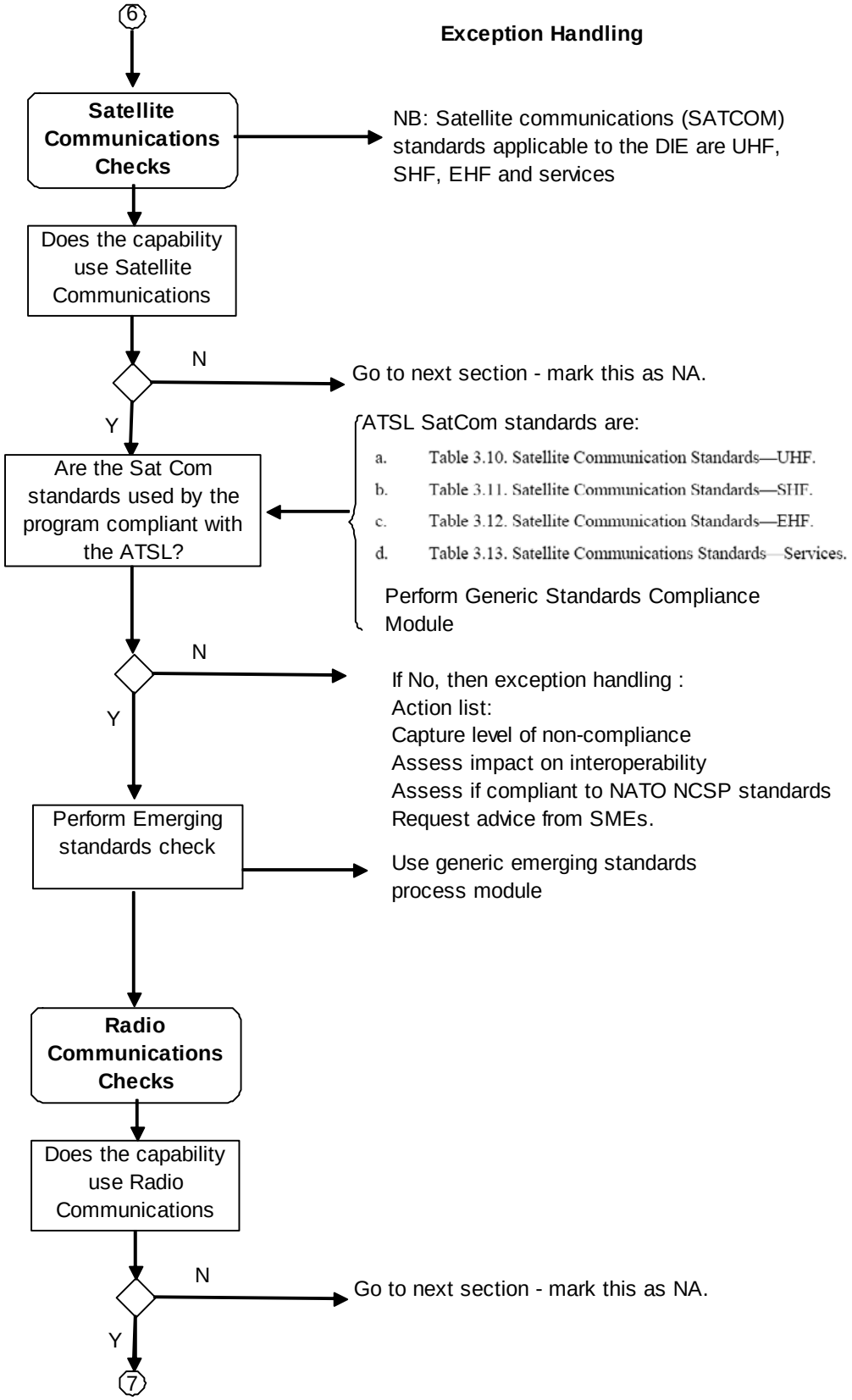
Net Readiness Example - Communications cont...



Net Readiness Example - Communications cont...

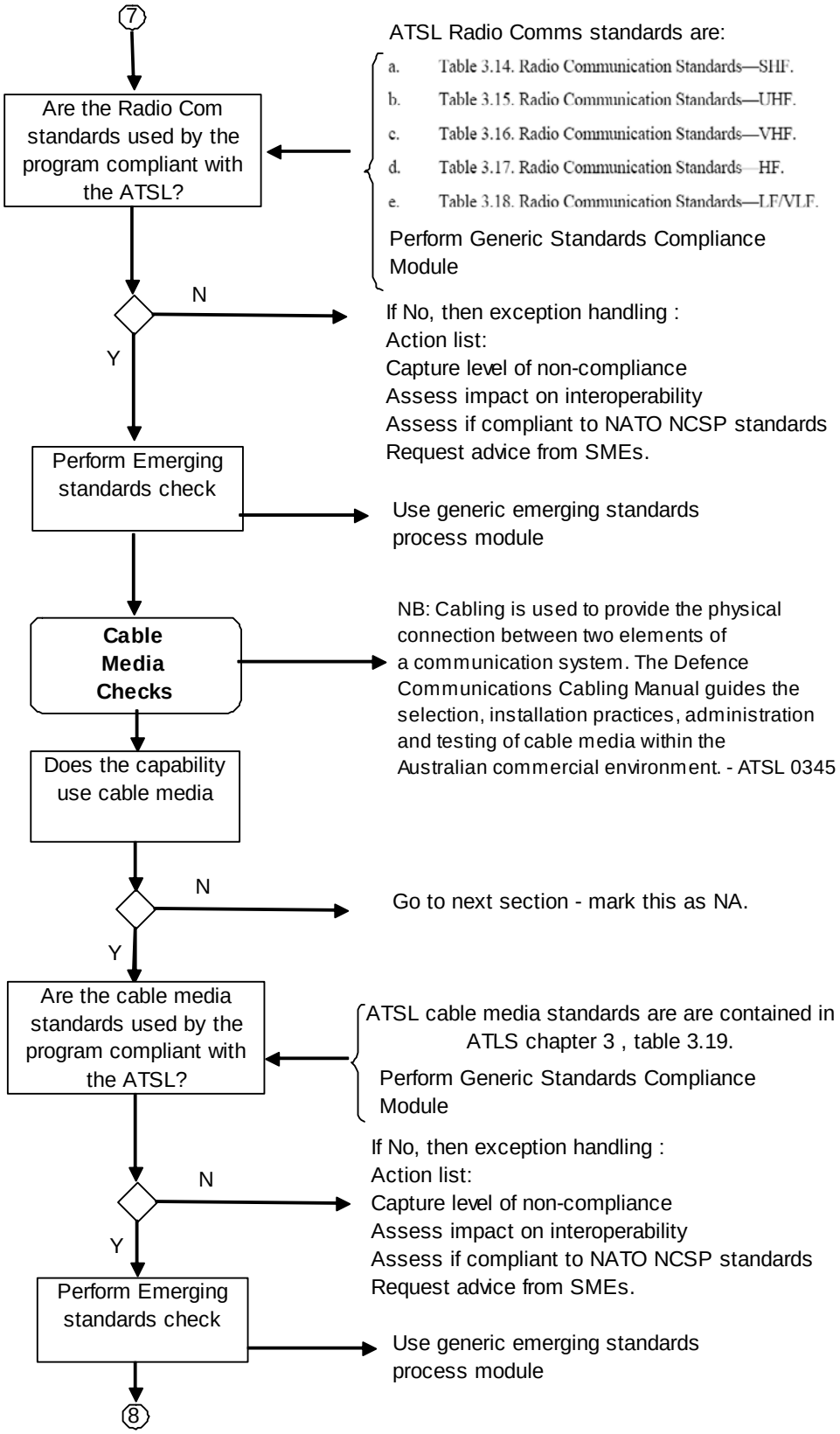


Net Readiness Example - Communications cont...

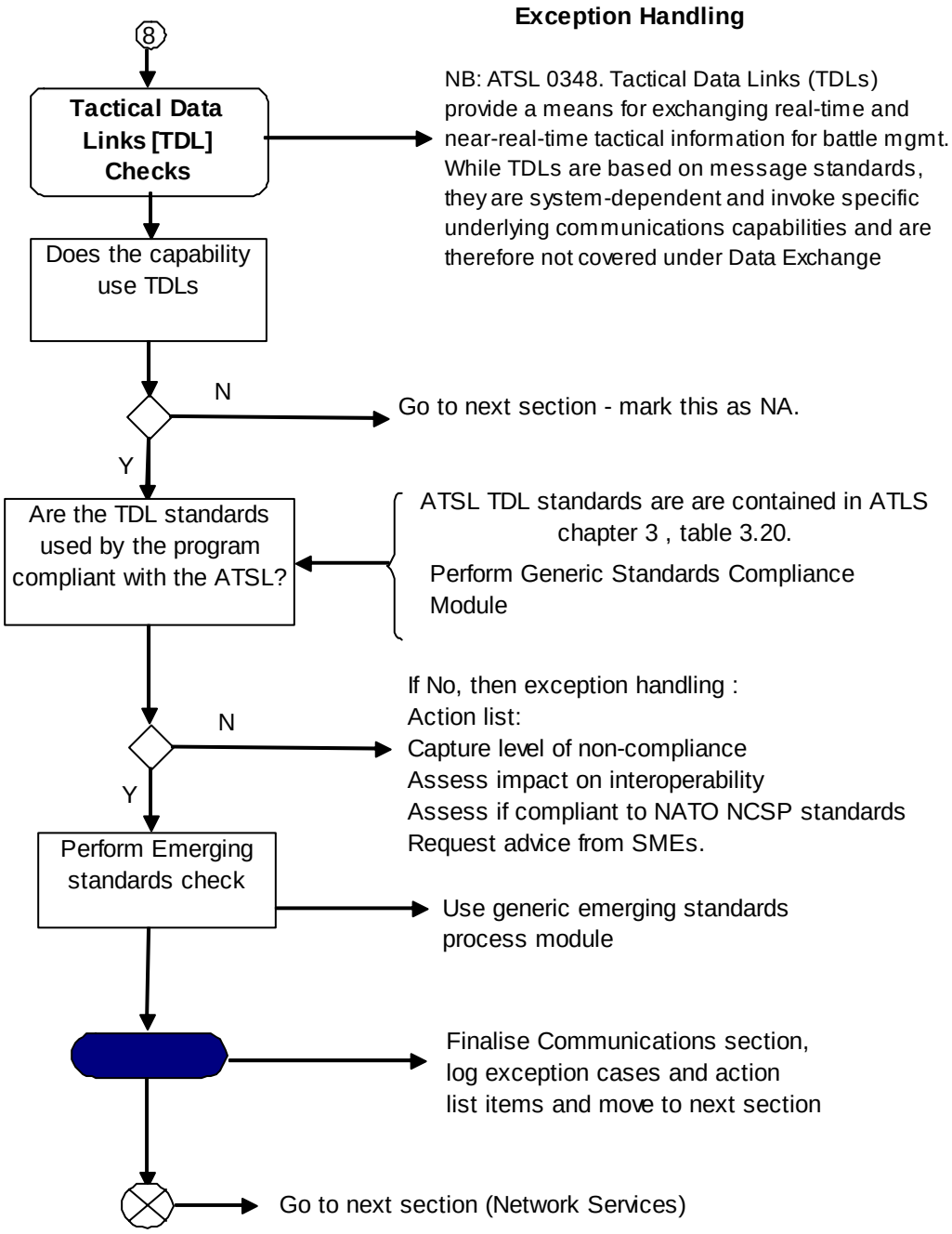


Net Readiness Example - Communications cont...

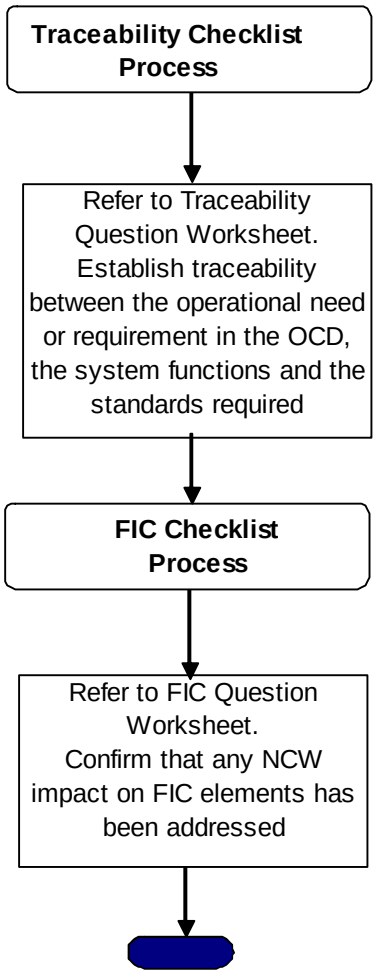
Exception Handling



Net Readiness Example - Communications cont...



B.7. Traceability and FIC Components



Appendix C: NCW Compliance Question List

This appendix provides a complete listing of all NCW Compliance questions that have been developed up to 31 March 2006, for each NCW Compliance Component.

The question list format includes a column for each of the following items:

- The input material or documentation that might be required to answer the question
- The NCW compliance question
- Exception handling if the answer to the compliance question is "No"
- Suggested reporting of the compliance issue in the First Pass documentation
- Suggested reporting of the compliance issue in the Second Pass documentation
- Action items to be addressed offline by the NCWPO support team
- Rationale for asking each question

C.1. NCW Priority Questions

Rationale: NCW Priority checks are used as a filter, to identify programs that need to be checked for NCW compliance. This will minimise the workload for desk officers and the NCWPO by enabling them to focus on high-payoff areas for NCW compliance.

Input material	Compliance Check	Exception handling	1st Pass Reporting	2nd Pass Reporting	Action List	Rationale for question
NCW Priority Questions						
Preliminary OCD	Will this project remain in service after 2015?					Determine whether the project will still be in service at a time when the ADF expects to be operating in an NCW environment [REF: NCW Roadmap 2005]
Preliminary OCD	Will this project require access to real-time or near-real-time information?					Identify projects for which NCW compliance will be important due to the requirement to exchange RT/NRT information
Preliminary OCD	Does this project include any Major Systems or Principal Items (eg vehicles, communications and training equipment)?					Major Systems and Principal Items should be NCW compliant
Preliminary OCD	Will this project provide any of the following functions and services? - Sensors or data collection - Information management, processing or analysis - C2 or decision-support - Weapons or effects - Logistics or resource management - Communications or networking					Identify projects with the potential to have a significant impact on NCW capability due to the type of functions and services they provide
	Did you answer YES to any of the NCW priority indicators above? - This indicates that the project may be an NCW Priority project and should be fully assessed for NCW compliance.	Seek confirmation from NCWPO that no further NCW Compliance Checking is required for this project	NCWPO certification that this is/is not an NCW Priority project	NCWPO certification that this is/is not an NCW Priority project - only for projects that are already through 1st Pass when first checked for NCW compliance		Every project should receive NCWPO certification that it has been checked for NCW Priority and stating whether further NCW Compliance Checking is required
NCW Roadmap	Is this project included in the NCW Roadmap?	Investigate why this NCW Priority project is not included in the NCW Roadmap			NCWPO to advise whether this project should appear in the NCW Raodmap and with what linkages and timeframes	NCW Priority projects should be included in the NCW Roadmap
NCW Integration Plan	Is this project included in the NCW Integration Plan?	Investigate why this NCW Priority project is not included in the NCW Implementation Plan			NCWPO to advise whether this project should appear in the NCW Implementation Plan and with what linkages and timeframes	NCW Priority projects should be included in the NCW Implementation Plan
1st Pass committee documentation	Has DNCWPO signed off on NCW priority?	Undertake any remedial action requested by NCWPO	1st Pass committee documentation includes NCWPO certification			Projects should not go to committee until the NCWPO has certified their NCW compliance status
2nd Pass committee documentation	Has DNCWPO signed off on NCW priority?	Undertake any remedial action requested by NCWPO		2nd Pass committee documentation includes NCWPO certification		Projects should not go to committee until the NCWPO has certified their NCW compliance status
	Did the NCW Compliance process assist you to determine the relevance of NCW issues to your project?	Please suggest improvements to the NCW Compliance Process			NCWPO to seek written or verbal feedback from desk officers	The NCW Compliance Process will be subject to continuous improvement

C.2. NCW Technical Interoperability Questions

Rationale: NCW Interoperability checks are used to ascertain whether the technical standards to be used by a project are compliant with those that are agreed for Defence - currently the agreed Defence standards appear in the DIE Approved Technical Standards List (ATSL). This check will enable any project to be assessed as being interoperable with existing systems within Defence as well as with potential ally nations who also mandate similar sets of approved standards. A similar check is done for emerging technical standards in situations where the technology is changing and a new standard has yet to be fully endorsed by an international body (eg ISO, IEEE, EIA).

Any discrepancy between the standards proposed by a project and those in the ATSL will require Exception Handling. This comprises an assessment of whether the proposed standard is compliant with international standards (eg NATO NCSP) and an assessment of the impact of any variances. The desk officer and NCWPO should seek advice from Subject Matter Experts (SME) as to what constraints any variances will impose on interoperability with other information systems within the DIE. SMEs may include members of the NCWPO Support Team, Capability Development Group, Office of the Chief Information officer (for DIE/ATSL advice) or External Service Providers (ESP) (for specialist technical advice).

Input material	Compliance Check	Exception handling	1st Pass Reporting	2nd Pass Reporting	Action List	Rationale for question
TRM, TV-1, TV-2 Questions						
Preliminary OCD, OCD, TV-1	Does the project documentation reference a Technical Reference Model (TRM)?	Default is to use the DIE ATSL.				All projects should identify the technical standards that they intend to implement. Ideally, these should be compatible with the DIE ATSL or future Defence TRM.
Preliminary OCD, OCD, TV-1	Is the project's Technical Reference Model compatible with the DIE ATSL? (Use ATSL Checklist to test for compliance)	Justify why a non-compliant TRM is used. State the impact of any variances. State whether the TRM is compliant with NATO NCSP.			NCWPO to assist the desk officer to check the TRM against the ATSL. Check any variances against NATO NCSP Seek advice from SMEs to assess the impact of any variances.	To determine if a TRM is referenced and if it is compatible with the DIE ATSL.
Preliminary OCD, OCD, TV-1	Does the capability have a TV-1 profile?	Justify why the mandated TV-1 has not been developed for the project, or develop the missing DAF product.	Preliminary OCD includes a TV-1	OCD includes a TV-1	NCWPO to assist the desk officer to check the OCD for any references to technical standards and develop a TV-1	TV-1 is the usual DAF product for stating the technical standards with which the project will conform
Preliminary OCD, OCD, TV-2	Does the capability have a TV-2 profile?	Justify why the mandated TV-2 has not been developed for the project, or develop the missing DAF product.	Preliminary OCD includes a TV-2	OCD includes a TV-2	NCWPO to assist the desk officer to check the OCD for any references to emerging technical standards and develop a TV-2	TV-2 is the usual DAF product for stating the emerging technical standards that the project intends to implement
OCD, TV-1, TV-2, RFP/RFT	Does the RFP/RFT include the project's TV-1 and TV-2 to provide a preferred technical profile for the project?	Justify why TV-1 and TV-2 are not used		RFP/RFT includes TV-1 and TV-2		Defence contractors should be encouraged to comply with Defence standards, or at least to provide a list of the standards used in their proposals and any variances from the ATSL (or future Defence TRM)

Input material	Compliance Check	Exception handling	1st Pass Reporting	2nd Pass Reporting	Action List	Rationale for question
ATSL Questions						
Preliminary OCD, OCD, TV-1, TV-2	Does the project use technical standards stated in the chapter heading of the ATSL?	If yes, then do compliance checks on the sub chapter topics, if not go to next chapter heading				Need to check if project uses technical standards that are endorsed for use within the DIE
Preliminary OCD, OCD, TV-1	Does the project use technical standards stated in the tables associated with each chapter sub heading within the ATSL?	If the proposed standards are compliant with those in the tables in the ATSL chapter sub heading - OK. If not, need to assess variance and impact on DIE of exception.			NCWPO to assist the desk officer to check for compliance with each entry of the ATSL table. Check any variances against NATO NCSP. Seek advice from SMEs to assess the impact of any variances.	ATSL chapter headings are broad categories of standards. If those categories are applicable, then the actual standards are stated in tables within chapter sub headings and it is these tables that are used for the compliance check
Preliminary OCD, OCD, TV-2	Does the project identify any emerging technical standards associated with each chapter sub heading within the ATSL?	Check if this is a logical decision or an oversight			NCWPO to seek advice from DSTO/DCG on emerging standards in this area	Identify any areas where there are emerging standards that could impact on this project
Preliminary OCD, OCD, TV-2	Are the emerging standards compliant with the ATSL?	If the proposed standards are compliant with those in the tables in the ATSL chapter sub heading - OK. If not, need to assess variance and impact on DIE of exception.			NCWPO to assist the desk officer to check for compliance with each entry of the ATSL table. Check any variances against NATO NCSP. Seek advice from SMEs to assess the impact of any variances.	Check that any emerging standards are compliant with the ATSL
1st Pass committee documentation	Has DNCWPO signed off on NCW interoperability?	Undertake any remedial action requested by NCWPO	1st Pass committee documentation includes NCWPO certification			Projects should not go to committee until the NCWPO has certified their NCW compliance status
2nd Pass committee documentation	Has DNCWPO signed off on NCW interoperability?	Undertake any remedial action requested by NCWPO		2nd Pass committee documentation includes NCWPO certification		Projects should not go to committee until the NCWPO has certified their NCW compliance status
	Did the NCW Compliance process assist you to assess technical standards and interoperability for your project?	Please suggest improvements to the NCW Compliance Process			NCWPO to seek written or verbal feedback from desk officers	The NCW Compliance Process will be subject to continuous improvement

C.3. ATSL Worksheet

The ATSL worksheet shown below provides a convenient way of summarising the results of the ATSL standards checking process.

ATSL Worksheet								
Input material	**ATSL Chapter Heading**	**ATSL Sub-Heading**	**Used in project? [Y/N]**	**Compliant with ATSL standards? [Y/N]**	**Migration plan for emerging standards? [Y/N]**	**Exception handling**	**Action List**	**Rationale for question**
Preliminary OCD, OCD, TV-1, TV-2, ATSL	**Operating Systems**							Check to ensure compliance with DIE operating systems
		2. DIE policy Table 2.1						
Preliminary OCD, OCD, TV-1, TV-2, ATSL	**Communications**							Check to ensure compliance with DIE Communication standards & protocols
		1. End to End Interconnection Protocols. Table 3.1						
		2. Local Area Networks (LANs). Table 3.2						
		3. Routers. Table 3.3						
		4. Wide Area Communications. Table 3.4 - 3.9						
		5. Satellite Communication (SATCOM). Table 3.10 - 3.13						
		6. Radio Communications. Table 3.14 - 3.18						
		7. Cable Media. Table 3.19						
		8. Tactical Data Links (TDLs). Table 3.20						
Preliminary OCD, OCD, TV-1, TV-2, ATSL	**Network Services**							Check to ensure compliance with DIE Network Services standards
		1. Messaging Service Table 4.1						
		2. Directory Service Table 4.2						
		3. Domain Name System (DNS) Table 4.3						
		4. Web Browser Service Table 4.5						
		5. Other Intranet/Internet Services Table 4.6						
		6. File Transfer and Access Service Table 4.7						
		7. Terminal Emulation Service Table 4.8						

Input material	ATSL Chapter Heading	ATSL Sub-Heading	Used in project? [Y/N]	Compliant with ATSL standards? [Y/N]	Migration plan for emerging standards? [Y/N]	Exception handling	Action List	Rationale for question
Preliminary OCD, OCD, TV-1, TV-2, ATSL	**Security**							Check for compliance with DIE Security standards
		1. General Security Services - General Table 5.1						
		2. General Security services - Authentication Table 5.2						
		3. General Security services - Access Control Table 5.3						
		4. General Security Services - Integrity Table 5.4						
		5. General Security services - Confidentiality Table 5.5						
		6. General Security services - Non-Repudiation Table 5.6						
		7. Messaging Security Services - Formal Table 5.7						
		8. Messaging Security Services - Informal (Email) Table 5.8						
		9. Web Services Security Table 5.9						
		10. Wireless Security Services Table 5.10						
		11. Boundary Protection Security Services – Firewalls Table 5.11						
		12. Boundary Protection Security Service–Content Checking Table 5.12						
		13. Public Key Infrastructure (PKI) Security Services Table 5.13						
		14. Audio-visual and Multimedia Security Services Table 5.14						
		15. Remote Access Security Services Table 5.15						
		16. Biometric Security Services Table 5.16						

Input material	ATSL Chapter Heading	ATSL Sub-Heading	Used in project? [Y/N]	Compliant with ATSL standards? [Y/N]	Migration plan for emerging standards? [Y/N]	Exception handling	Action List	Rationale for question
Preliminary OCD, OCD, TV-1, TV-2, ATSL	**User Interface**							Check for compliance with DIE User Interface standards
		1. Graphical Client/Server Operations Table 6.1						
		2. Object Definition and Management Services Table 6.2						
		3. Window Management Specifications. Table 6.3						
Preliminary OCD, OCD, TV-1, TV-2, ATSL	**Data Management**							Check for compliance with DIE Data Management standards
		1. Data Management Reference Models and Frameworks Table 7.1						
		2. Management of Data Table 7.2						
		3. Information Management Table 7.3						
		4. Database Management Table 7.4						
		5. Data Access Table 7.5						
Preliminary OCD, OCD, TV-1, TV-2, ATSL	**Data Exchange**							Check for compliance with DIE Data Exchange standards
		1. Document Exchange Table 8.1						
		2. Business Data Exchange Table 8.2						
		3. Military Data Exchange Table 8.3						
		4. Encoding and Character Sets Table 8.4						
		5. Facsimile Table 8.5						
		6. Geospatial Data Exchange Table 8.6						
		7. Multimedia – Static Content Exchange Table 8.7						
		8. Multimedia – Dynamic Content Exchange Table 8.8						

Input material	ATSL Chapter Heading	ATSL Sub-Heading	Used in project? [Y/N]	Compliant with ATSL standards? [Y/N]	Migration plan for emerging standards? [Y/N]	Exception handling	Action List	Rationale for question
Preliminary OCD, OCD, TV-1, TV-2, ATSL	**Graphics**							Check for compliance with DIE graphics standards
		1. Raster Graphics Table 9.1						
		2. Vector Graphics Table 9.2						
		3. Device Interfaces Table 9.3						
Preliminary OCD, OCD, TV-1, TV-2, ATSL	**Network & System Management**							Check that services offered for network, system and information management are compliant with DIE requirements.
		1. Configuration Management Table 10.1						
		2. Incident Management Table 10.2						
		3. Problem Management Table 10.3						
		4. Change Management Table 10.4						
		5. Service/Help Desk Table 10.5						
		6. Release Management Table 10.6						
		7. Service Level Management Table 10.7						
		8. Capacity Management Table 10.8						
		9. Continuity Management Table 10.9						
		10. Availability Management Table 10.10						
		11. IT Financial Management Table 10.11						
		12. Deployed NSM Table 10.12						
		13. Access Control Table 10.13						

Input material	ATSL Chapter Heading	ATSL Sub-Heading	Used in project? [Y/N]	Compliant with ATSL standards? [Y/N]	Migration plan for emerging standards? [Y/N]	Exception handling	Action List	Rationale for question
Preliminary OCD, OCD, TV-1, TV-2, ATSL	**Distributed Computing**							Checks to ensure that services provides in a distributing computing environment are compliant with the DIE standards
		1. Technological Overview Table 11.1						
		2. Distributed environment Table 11.2						
		3. Distributed Remote Process Services Table 11.3						
		4. Distributed Time Services Table 11.4						
		5. Distributed Object Services Table 11.5						
		6. Distributed Simulation Table 11.6						
Preliminary OCD, OCD, TV-1, TV-2, ATSL	**Software Engineering**							Check to ensure compliance with DIE standards, tools, languages and methodologies for software development.
		1. SE Terminology Table 12.1						
		2. SE Management Table 12.2						
		3. Software Life-Cycle Table 12.3						
		4. SE Documentation Table 12.4						
		5. SE Quality Table 12.5						
		6. Languages and API/Bindings Table 12.6						
		7. CASE Tools Table 12.7						

C.4. NCW Traceability Questions

Rationale: All projects should support the ADO's future warfighting objectives. Systems and operations analysis is required to develop (from policy guidance) a set of Endorsed NCW Principles and Target States that can be checked at the individual project level. Desk officers will be able to demonstrate that their projects support higher-level NCW guidance, by listing the NCW Principles and Target States that the project will support, and demonstrating that there is traceability through the project documentation, including the Defence Architecture Framework (DAF) products that are part of the Operational Concept Document (OCD).

Input material	Compliance Check	Exception handling	1st Pass Reporting	2nd Pass Reporting	Action List	Rationale
NCW Traceability - Preliminary Documentation Checks						
Preliminary OCD, Endorsed NCW Principles & Target States (TBD)	State the NCW Principles that this project supports	Justify why the project does not support the other NCW Principles	Preliminary OCD includes a list of Supported NCW Principles			NOTE: these checks to be refined when the NCWPO has an endorsed set of NCW Principles.
Preliminary OCD, Preliminary FPS	?List those operational activities that relate to each of the Supported NCW Principles	Justify why any of the Supported NCW Principles do not have an associated operational activity	Preliminary FPS includes a list of operational activities traceable to the Supported NCW Principles			
Preliminary OCD, Preliminary FPS	?List those system functions that relate to each of the NCW-related operational activities	Justify why any of the NCW-related operational activities do not have an associated system function	OCD includes a list of system functions traceable to the operational activities and Supported NCW Principles			
Ist Pass committee documentation	Has DNCWPO signed off on NCW traceability?	Undertake any remedial action requested by NCWPO	Ist Pass committee documentation includes NCWPO certification			Projects should not go to committee until the NCWPO has certified their NCW compliance status
NCW Traceability - Final Documentation Checks						
OCD, Preliminary OCD, Endorsed NCW Principles & Target States (TBD)	Does the project still support the NCW Principles identified in the Preliminary OCD?	Justify any changes		OCD includes a list of Supported NCW Principles		
OCD, FPS	?Are the Supported NCW Principles still associated with at least one operational activity?	Justify any changes		FPS includes a list of operational activities traceable to the Supported NCW Principles		
OCD, FPS	?Are the NCW-related operational activities still associated with at least one system function?	Justify any changes		OCD includes a list of system functions traceable to the operational activities and Supported NCW Principles		
OCD, FPS	List those standards that are associated with each of the NCW-related system functions	Justify why any of the NCW-related system functions do not have an associated technical standard		OCD includes a list of technical standards traceable to the system functions, operational activities and Supported NCW Principles		
OCD, FPS, RFP/RFT	?List those RFT/RFP requirements that relate to each of the NCW-related system functions	Justify why any of the NCW-related system functions do not have an associated RFP/RFT requirement		RFP/RFT includes requirements that are traceable to the system functions, operational activities and Supported NCW Principles		
2nd Pass committee documentation	Has DNCWPO signed off on NCW traceability?	Undertake any remedial action requested by NCWPO		2nd Pass committee documentation includes NCWPO certification		Projects should not go to committee until the NCWPO has certified their NCW compliance status
	Did the NCW Compliance process assist you to incorporate NCW guidance in your project?	Please suggest improvements to the NCW Compliance Process			NCWPO to seek written or verbal feedback from desk officers	The NCW Compliance Process will be subject to continuous improvement

C.5. NCW FIC Questions

Rationale: All projects should identify and address any NCW impact on FIC elements. This section picks up FIC items not already covered elsewhere in the NCW Compliance Process. It aims to ensure that project documentation describes how NCW impact on FIC elements will be addressed (where applicable).

Input material	Compliance Check	Exception handling	1st Pass Reporting	2nd Pass Reporting	Action List	Rationale for Question
NCW Fundamental Inputs to Capability (FIC) Checks						
Endorsed NCW Principles & Target States (TBD), Preliminary OCD, OCD	Will the project's organisational or command structure support each of the endorsed NCW Principles & Target States (eg flexible functional groupings)?	Justify why the organisational structure for the project will not support each of the endorsed NCW Principles or prepare missing project documentation	OCD describes how the organisational structure will support each of the endorsed NCW Principles	OCD describes how the organisational structure will support each of the endorsed NCW Principles		FIC Organisation: Organisational structure needs to support NCW tenets (eg self-synchronisation, flexible functional groupings) NOTE: these checks to be refined when the NCWPO has an endorsed set of NCW Principles.
OCD, FPS, RFP/RFT	Has this project identified its NCW-compliant technology requirements? (eg communications and IT equipment)	Justify why there is no requirement for NCW-compliant technology or prepare the missing documentation			NCWPO to assist the desk officer to identify NCW-compliant technologies relevant to the project	FIC Personnel: Require individuals who are trained in the use and administration of NCW-compliant IT and other military equipment
Preliminary OCD, OCD	Does the project documentation identify specific personnel requirements, staffing numbers and competencies for operating in an NCW environment?	Justify why there are no specific NCW-related personnel requirements or prepare the missing documentation	Preliminary OCD identifes the NCW-related personnel requirements	OCD identifes the NCW-related personnel requirements		FIC Organisation & Personnel: Need people who are competent to operate in an NCW environment.
Preliminary OCD, OCD	Does the project documentation describe how any NCW-related personnel requirements will be addressed?	Justify why there is no plan for addressing any NCW-related personnel requirements or prepare the missing documentation	Preliminary OCD includes a plan for addressing any NCW-related personnel requirements	OCD includes a plan for addressing any NCW-related personnel requirements		FIC Organisation, Personnel & Support: Need people who are competent to operate in an NCW environment. Need to attract, train & retain people who prefer to operate in an NCW environment.
OCD, RFP/RFT	Has this project made provision for individual training on any NCW-compliant technologies identified above?	Justify why there is no provision for individual training on NCW-compliant technologies or prepare the missing documentation		OCD, RFP/RFT includes provision for individual training on NCW-compliant technologies		FIC Personnel: Require individuals who are trained in the use and administration of NCW-compliant IT and other military equipment
Preliminary OCD, OCD	Has this project made provision for collective training in NCW environments?	Justify why there is no provision for collective training in NCW environments or prepare the missing documentation	Preliminary OCD includes provision for training in NCW environments	OCD includes provision for training in NCW environments	NCWPO to identify appropriate training or experimentation environments as part of a follow-on NCW Compliance work program	FIC Collective Training: Essential that all types of collective training include operations in NCW environments
OCD, FPS, RFP/RFT	Has this project identified facilities and infrastructure to support the NCW-compliant technology requirements identified above? (eg buildings, utilities, training facilities)	Justify why no special infrastructure is required to support any NCW-compliant technology or prepare the missing documentation		OCD includes an infrastructure strategy for supporting NCW-compliant technology requirements		FIC Facilities: Need to ensure there is sufficient and adequate infrastructure for IT & communications and the capability to test NCW-compliant equipment & doctrine

Input material	Compliance Check	Exception handling	1st Pass Reporting	2nd Pass Reporting	Action List	Rationale for Question
OCD, FPS, RFP/RFT	Has this project identified an operating and support strategy for the NCW-compliant technology and infrastructure requirements identified above?	Justify why no special operating and support strategy is required for any NCW-compliant technology and infrastructure or prepare the missing documentation		OCD includes an operating and support strategy for NCW-compliant technology and infrastructure		FIC Facilities: Need appropriate equipment and personnel to support NCW compliant communications & IT capabilities. Need to consider NCW impact on support procedures (eg impact of taking equipment offline for maintenance)
OCD, FPS, RFP/RFT	Has this project identified a supply strategy for the NCW-compliant technology requirements identified above? (eg communications and IT equipment)	Justify why no special provisions are required to maintain supply of any NCW-compliant technology or prepare the missing documentation		OCD includes a supply strategy for NCW-compliant technology requirements		FIC Supplies: Where NCW compliance has imposed a requirement for specialised parts and components, special consideration should be given to maintaining supply. Need to consider how parts will be sourced – eg are certain NCW-compliant parts only available from the US? What is the lead-time and availability? Will Australia stock spares? Will we rely on US to supply in time of war?
Preliminary OCD, OCD	Has this project identified its requirements for support from the wider national support base within Australia and offshore?	Justify why there is no requirement for support or prepare the missing documentation		OCD includes a strategy for obtaining support from the wider national support base		FIC Support & Organisation: need to support NCW tenets (eg whole-of-nation approach) NOTE: these checks to be refined when the NCWPO has an endorsed set of NCW Principles.
Preliminary OCD, OCD	Has this project identified a requirement to exchange information with other Government and international agencies?	Justify why there is no requirement to exchange information with other agencies or prepare the missing documentation		OCD includes a strategy for exchanging information with other agencies		FIC Support & Organisation: need to support NCW tenets (eg whole-of-nation approach) NOTE: these checks to be refined when the NCWPO has an endorsed set of NCW Principles.
Preliminary OCD, OCD	Does this system use, produce or provide intelligence?	Justify why this system does not use, produce or provide intelligence	Preliminary OCD describes the project's intelligence mangement strategy and how it will support endorsed NCW Principles	OCD describes the project's intelligence management strategyand how it will support endorsed NCW Principles		FIC Support & Organisation: need to support NCW tenets which might require new intelligence models (eg distributed analysis) NOTE: these checks to be refined when the NCWPO has an endorsed set of NCW Principles.
Preliminary OCD, OCD	Has this project identified a requirement for any NCW-related studies or R&D?	Justify why the project has no requirement for NCW-related studies or prepare the missing documentation				FIC Support & Organisation: R&D studies may be required to explore NCW tenets NOTE: these checks to be refined when the NCWPO has an endorsed set of NCW Principles.

Input material	Compliance Check	Exception handling	1st Pass Reporting	2nd Pass Reporting	Action List	Rationale for Question
Preliminary OCD, OCD, doctrine and procedures	Does the project documentation identify NCW-related impacts on doctrine and procedures?	Justify why the project will have no NCW-related impact on doctrine and procedures or prepare the missing documentation				FIC Cmd&Mgmt: Doctrine, decision-making processes, tactical-level procedures and risk management need to support NCW tenets (eg self-synchronisation) NOTE: these checks to be refined when the NCWPO has an endorsed set of NCW Principles.
OCD	Does the project documentation describe how this system will be tested in an NCW environment?	Do nothing until the NCWPO has completed further work on NCW testing			NCWPO to identify appropriate training or experimentation environments as part of a follow-on NCW Compliance work program	FIC Collective Training & Facilities: Need to ensure there is the capability to test NCW-compliant equipment & doctrine in suitable test environments NOTE: these checks to be refined when the NCWPO has an endorsed set of NCW Principles.
NCWPO to consider the inclusion of the following questions when a set of NCW Principles has been endorsed: What processes will be established to enable decentralised planning and operations? What processes will be established to encourage decision-makers to collaborate? What processes will be established to enable other agencies to influence the planning process/priorities? What processes will be established to enable other agencies to influence the tasking process/priorities? What processes will be established to enable other agencies to influence the data collection process/priorities? What processes will be established to involve other agencies and allies in collective training? What processes will be established to make data and information available to other users? What processes will be established to make the data/information discoverable by other users (eg inclusion of metadata)? What processes will be established to make the data/information useable by other users (eg inclusion of pedigree metadata)? What processes will be established to manage remote access to the system? What processes will be established to maintain information security? What processes will be established to encourage learning and adaptation? What processes will be established to measure and improve the timeliness and quality of the delivered capability's performance?						
1st Pass committee documentation	Has DNCWPO signed off on NCW FIC?	Undertake any remedial action requested by NCWPO	1st Pass committee documentation includes NCWPO certification			Projects should not go to committee until the NCWPO has certified their NCW compliance status
2nd Pass committee documentation	Has DNCWPO signed off on NCW FIC?	Undertake any remedial action requested by NCWPO		2nd Pass committee documentation includes NCWPO certification		Projects should not go to committee until the NCWPO has certified their NCW compliance status
	Did the NCW Compliance process assist you assess the impact of NCW guidance on the FIC for your project?	Please suggest improvements to the NCW Compliance Process			NCWPO to seek written or verbal feedback from desk officers	The NCW Compliance Process will be subject to continuous improvement

Appendix D: NCW Priority Component

The purpose of the NCW Priority Component is to identify any projects that do not need to proceed to full NCW Compliance Assessment. This filtering is intended to reduce the workload for desk officers and NCWPO staff by allowing them to focus on those projects that are expected to have a high impact on the ADO's future NCW capability.

Factors that are checked by the NCW Priority process include:

- **Timeframe**: whether the project will be withdrawn from service before 2015, i.e. whether the project will still be in service at a time when the ADF expects to be operating in an NCW environment (2015 is the point of reference used in the NCW Roadmap 2005) [CDG 2005]
- **Timeliness of information flows**: whether the project has a requirement to exchange real-time or near-real-time information
- **Major systems, functions and services**: whether the project will deliver major systems that provide a significant C3I, sensing, effects or logistics capability

Projects with at least one indicator in each category should be assessed for Net-readiness and should be considered for inclusion in the NCW Roadmap and Integration Plan (if not already included). Other projects should be provided with a copy of the NCW assessment material for their consideration and information, but no formal NCW Compliance checks would be undertaken.

Appendix E: NCW Traceability Component

All projects should support the ADO's future warfighting objectives. Systems and operations analysis is required to develop (from policy guidance) a set of endorsed NCW Principles and Target States that can be checked at the individual project level. Desk officers will be able to demonstrate that their projects support higher-level NCW guidance, by listing the NCW Principles and Target States that the project will support, and demonstrating that there is traceability through the project documentation, including the Defence Architecture Framework (DAF) products that are part of the Operational Concept Document (OCD).

Compliance Stage	**First Pass**
Reference material	Prelim OCD (including DAF products), Prelim FPS
Compliance Questions	– Which of the NCW Principles and Target States will this project support? – List those operational activities that relate to each of the supported NCW Principles identified above – List those system functions that relate to each of the operational activities identified above
Exception Handling	Justify why the project will not support the other NCW Principles
Compliance Stage	**Second Pass**
Reference material	OCD (including DAF products), FPS, RFT/RFP
Compliance Question	– List those operational activities that relate to each of the supported NCW Principles identified above (check new documentation) – List those system functions that relate to each of the supported NCW Principles identified above (check new documentation) – List those standards that are associated with each of the NCW-related system functions – List those RFT/RFP requirements that relate to each of the system functions identified above
Exception Handling	Justify why the project will not support the other NCW Principles (for any NCW Principles that have been dropped from later drafts of the documentation or where traceability has not been demonstrated)

For convenience, the NCWPO might choose to record NCW Traceability in a table such as:

#	NCW Principle	Supported?	Related Operational Activities	Related System Functions	Related RFT/RFP Req'ments	Exception handling
1.1	Name/description of NCW Principle 1.1	Y/N				Justification for not supporting this NCW Principle
1.2						

Appendix F: NCW Interoperability Component

Before a capability can be introduced into the future Netforce, it needs to exhibit some basic characteristics such as technical interoperability with other components of the Netforce. In a net-centric environment, a capability may be required to interface with different systems belonging to Australia or coalition partners, whose interface details can not be specified beforehand. Hence an approach is required that does not rely on prior knowledge of specific interfaces but permits an assessment of technical interoperability compliance to be made.

The NCW Compliance Process adopts a standards-based approach to assess the level of technical interoperability of a proposed capability in a net-centric environment. Ideally, a Technical Reference Model (TRM) would be developed to define a common set of interoperability standards for the future Netforce (Appendix A.3). In the absence of a TRM, NCW Compliance would be evaluated against the core set of standards mandated for the Australian DIE; namely, the Australian Technical Standards List (ATSL). This core set of standards aims to define the target technical environment for the acquisition, development, and support of Defence information and communications technology systems.

F.1. ATSL

> *"The ATSL is the principal reference for Defence single service, joint and combined interoperability standards. While the ATSL is under development there will be a number of technology standards areas for which standards have not yet been mandated. These standards areas are readily identifiable by the chapter "interim guidance" sheets in the ATSL which advise the information shown in paragraph 113. 0113. Until a relevant chapter of the ATSL is published the precedence for sourcing standards is:*
>
> 1. ***Joint or Combined Interoperability.*** *Refer to the latest version of Allied Data Publication 34 Volume 4 (ADatP 34 Vol 4) NATO C3 Common Standards Profile (NCSP)*
> 2. ***Joint or Combined Interoperability that is not covered in the NCSP.*** *Refer to the latest version of the United States Department of Defence Joint Technical Architecture (US DoD JTA). The US DoD JTA should also be consulted for other than interoperability standards.*
> 3. ***Commonwealth Government Interoperability Standards.*** *When interoperability with other Commonwealth Federal Agencies is a requirement, refer to the latest version of the Interoperability Framework for the Commonwealth Government. (See http://www.noie.gov.au)."* [CIO 2005]

The DIE ATSL covers the following technology standards areas [CIO 2005]:

a. Operating Systems;
b. Communications;
c. Network Services;
d. Security;
e. User Interface;

f. Data Management;
g. Data Exchange;
h. Graphics;
i. Network and System Management;
j. Distributed Computing (NEC/NCW related services), and
k. Software Engineering.

F.2. Technical Interoperability Compliance Process

The NCW Technical Interoperability Component uses a set of questions (Appendix C) to guide the reviewer in assessing whether or not the proposed capability specifies and conforms with the technical standards in the DIE ATSL. The process requires the reviewer to examine the capability's documentation set. In particular, the DAF TV-1 product in the capability's OCD provides a list of relevant technical standards to be utilised in the development of the capability's technical architecture. DAF TV-2 specifies any emerging standards that are relevant to the capability project.

At the Fist Pass stage, the draft TV-1 and TV-2 (if available) would be assessed against the ATSL. At the Second Pass stage, detailed DAF products should be available including a TV-1. At this point, a comprehensive comparison of the TV-1 against the ATSL should be possible. Any variances are to be handled as an exception report. The TV-2 (if available) should be checked for compliance of emerging standards. In future, at the Second Pass stage, company responses to RFP/RFTs might be checked to determine whether they comply with mandated technical standards.

The NCW Compliance questions guide the reviewer through each chapter of the ATSL to determine:

1. Whether each chapter and sub-section is relevant to the project and
2. Whether the project documentation specifies standards that are consistent with those in the ATSL.

An Exception Handling process is used to capture any variances between a project's proposed technical standards and those referenced within the ATSL. The exception handling process comprises the logging of the variances, assessment of further analysis required to resolve the variances and compilation of an action list to reflect such activities. If the TV-1 is incomplete, then an exception report is generated. If standards are specified in the TV-1 that do not appear in the ATSL, then the NATO NCSP or the US DOD JTA may be checked and an exception report would be generated, noting that theTV-1 standard did not appear in the ATSL and requires further consideration. If the tender requirements documentation (eg RFP/RFT) fails to include technical standards, then an exception report should be generated. If a proposed solution fails to comply with required technical standards, or proposes to comply with different standards (eg US or NATO standards instead of the ATSL), then an exception report should also be generated.

A report is produced stating the level of compliance, with exception reports where variances were noted.

F.3. Technical Interoperability Assumptions and Constraints

1. The Technical Interoperability assessment is based on standards compliance and is not intended to be an independent interoperability assessment process
2. Aspects associated with the physical integration of the capability and the Netforce will not be considered (eg compatibility of hardware connectors, cables, LAN wiring, etc). Except where relevant standards are explicitly addressed in the ATSL, this is an assembly and integration task left to the capability contractor
3. Aspects associated with the integration of information and communication technologies will be assessed
4. The DIE ATSL [CIO 2005] is the primary reference
5. The NATO NCSP [NATO 2006] is a secondary reference
6. In order to undertake this assessment, the reviewer will require access to the CDG project documentation (primarily the OCD), the DIE ATSL and secondary references
7. The quality of the assessment will be directly dependent on the level of detail within the CDG project documentation – in particular the TV-1 and TV-2 DAF products
8. In the case of complex systems being evaluated, the reviewer may need to request the assistance of an experienced systems engineer.

The list of proposed NCW Technical Interoperability questions is provided in Appendix C.

Appendix G: NCW FIC Component

G.1. Fundamental Inputs to Capability Overview

The Fundamental Inputs to Capability (FIC) is the standard list for consideration of what is required to generate 'capability'. The list is used by ADO agencies at all levels and is designed to ensure that all agencies manage and report capability using a common set of management areas. This not only assists with the allocation of financial resources across Defence and improves accountability, but enhances the formulation of a response to a contingency, when it arises thus directly impacting on the assembly and deployment of a net-centric Joint or Combined Task Force. The following information describes each element of the FIC [DEFWEB 2006].

Organisation Every ADO agency needs to ensure it has the required personnel establishment, appropriate balance of competency/skill-sets, and correct structure to accomplish its tasks and to ensure adequate command and control. This is essentially a minimal cost activity that provides the underpinning structure for Defence. At the Service level, consideration must be given to developing flexible functional groupings that can meet contingency personnel rotation requirements and continual force improvement requirements.

Personnel Positions in an authorised establishment must be filled by individuals who satisfy the necessary individual readiness requirements. Requirements include medical/dental standards, physical fitness and appropriate individual training. Each individual must have the competencies to perform the functions of their positions (both specialist and common military skills) and the motivation to apply those competencies to achieve the required performance standards of the organisation. The personnel element includes the retention and development of people to meet Defence's needs. This category includes salaries and wages, superannuation and allowances.

Collective Training applies across Combined, Joint, Single Service and unit levels. To enhance performance, organisational elements must undertake a comprehensive and on-going collective training regime validated against the preparedness requirements derived from Government guidance.

Major Systems are those that have a unit cost of A$1m or more, and/or have significant Defence policy or Joint Service implications. They include ships, tanks, missile systems (eg Air Defence batteries), armoured personnel carriers, major electronic systems (eg JORN and JCSE), and aircraft. While there is an apparent linkage with Class 7 Supplies, major systems are core components of capability that regularly require more detailed reporting and management, and will be considered separately.

Supplies ADFP 20 [1999] specifies 11 classes of supply (consistent with NATO). For many items, there is a need to identify more than just quantities (e.g. serviceability, configuration status, operational viability resources and reserve stockholdings). The 11 classes are:

- *Class 1: Subsistence*, including foodstuffs, gratuitous health, welfare items, and water when this is provided in a packaged form through the supply system.
- *Class 2: General Stores*, including clothing, individual equipment, tentage, tool sets and kits, hand tools, stationery and other general administrative and household items.
- *Class 3: Petrol, Oils and Lubricants (POL)*, including other hazardous liquids, chemicals and gases such as LPG and hexamine.
- *Class 4: Construction Items*, and materials and all fortification and barrier materials, excluding explosive devices.
- *Class 5: Ammunition*, including precision-guided munitions (PGMs), pyrotechnics, propellants and fuses.
- *Class 6: Personal Demand Items*, including canteen supplies and non-scaled military items.
- *Class 7: Principal Items*. This excludes major systems as described above. This class constitutes a combination of end products ready for their intended use, such as most vehicles, small arms, communications equipment and training equipment.
- *Class 8: Medical and Dental Stores.*
- *Class 9: Repair Parts and Components.*
- *Class 10: Miscellaneous*, also known as materiel support to non-military programs.
- *Class 11: Controlled Stores* (Quadripartite forum only).

Facilities including buildings, structures, property, plant and equipment, and areas for training and other purposes (eg exercise areas and firing ranges), utilities and civil engineering works necessary to support capabilities, both at the home station and at a deployed location. This may involve direct ownership or leasing arrangements.

Support A widely embracing category that encompasses the wider National Support Base and includes training/proficiency support, materiel/maintenance services, communications/IT support, intelligence, recruiting/retention, research and development activities, administrative support and transportation support. Agencies that could provide this support include:

- Other Sub-Outputs
- Output Enablers
- Owner Support agencies
- Civil/Private Industry/Contractors
- Other Government agencies (eg DHA)
- International Support Base agencies.

Command and Management underpin Defence operating and management environments through enhanced command and decision-making processes/procedures and management reporting avenues. Command and management processes at all levels are required to plan, apply, measure, monitor, and evaluate the functions an agency performs, with due cognisance of risk and subsequent risk management. Command and Management include written guidance such as regulations, instructions, publications, directions, requirements, doctrine, tactical-level procedures, and preparedness documents. Consideration must be given to the adequacy of extant written guidance.

G.2. Aspects of the FIC that relate to NCW Compliance

The focus for NCW compliance is on Major Systems as these will define the core capabilities from which a net-centric Joint Task Force would be assembled. For analysis of net-readiness, consideration should also be given to (in roughly descending order):

- *Organisation* but focussing on structure and processes
- *Command and Management*, particularly concepts and doctrine, decision-making processes, tactical-level procedures and risk management
- *Facilities*, with an emphasis on incorporation of sufficient and adequate infrastructure for IT and communications. Also of interest may be facilities for training in net-centric environments
- *Support*, particularly communications and IT support, intelligence and an ability to use national and international assets and capabilities
- *Supplies (Class 7)* where the capability uses or has implications for precision-guided munitions (PGM)
- *Personnel* as it relates to the skills base needed to undertake net-centric operations
- *Collective training*, particularly joint service training.

Aspects of *Personnel* such as medical standards, salaries, superannuation and allowances are unlikely to have a significant and direct effect on the net-readiness of Defence capabilities. Apart from PGMs included under *Ammunition*, the 10 classes of *Supply* are unlikely to have a direct bearing on the achievement of net-readiness. Aspects of *Organisation* other than structure and processes are also unlikely to have a major bearing on net-centric operations.

The NCW FIC Analysis elements identified here appear to correspond closely to the five prime elements of the UK's network-enabled capability (NEC) where *Personnel* and *Collective Training* are identified in both schema; *Major Systems* corresponds to the UK's *Equipment* element and *Command & Management* to the UK's *Concepts and Doctrine* [Dstl 2004]. It is not, however, clear where in the Australian FIC the UK *Structures and Processes* element would fit. In the proposed FIC approach, *Structures* and *Processes* are included under *Organisation*.

FIC analysis for NCW compliance will be undertaken by establishing a suitable list of questions for the secondary FIC (as identified above) to augment the primary NCW Compliance checks for *Major Systems*. The main problem is to identify cross-FIC interactions and situations where an issue with one of the secondary FIC could prevent a capability from achieving net-readiness or disrupt the integration of a major system into a net-centric Joint or Combined Task Force.

G.3. NCW FIC Profile

The following NCW FIC Profile is based on the above considerations. It includes only those FIC elements that are deemed to be relevant to NCW. This NCW FIC profile is used as the basis for the NCW FIC Compliance Questions in Appendix C.

Table 2 NCW FIC Profile (shaded elements)

FIC element	FIC sub-element		Relevance to NCW FIC Profile
Organisation	Structure	✓	Organisational structure needs to support NCW tenets (eg self-synchronisation, flexible functional groupings)
Organisation	Personnel establishment, balance of competency/skill-sets	✓	Need people who are competent to operate in an NCW environment
Personnel	Individual training	✓	Require individuals who are trained in the use and administration of NCW-compliant IT and other military equipment
Personnel	Medical/dental standards, physical fitness, salaries & wages, superannuation & allowances	×	
Collective training	Combined, Joint, Single Service and unit levels	✓	Essential that all types of collective training include operations in NCW environments
Major Systems	Ships, tanks, missile systems, armoured personnel carriers, major electronic systems, aircraft	✓	These should be NCW compliant
Supplies	Principal items (vehicles, small arms, communications and training equipment) and controlled stores (such as cryptographic equipment)	✓	These should be NCW compliant
Supplies	Repair parts and components	✓	Need to consider how parts will be sourced – eg are certain NCW-compliant parts only available from the US? What is the lead-time and availability? Will Australia stock spares? Will we rely on US to supply in time of war?
Supplies	Subsistence, General Stores, Petrol, Oils and Lubricants, Construction items, Ammunition, Personal demand items, Medical and dental stores, Miscellaneous	×	
Facilities	Buildings, structures, property, plant & equipment, utilities, civil engineering works, training areas, firing ranges	✓	Might need to be designed/modified for NCW compliance (eg adequate infrastructure for IT & communications, capability to test NCW-compliant equipment & doctrine)
Support	Training, proficiency, recruiting, retention support	✓	Need to attract, train & retain people who prefer to operate in an NCW environment
Support	Materiel, maintenance, communications, IT services	✓	Need appropriate equipment and personnel to support NCW compliant communications & IT capabilities. Need to consider NCW impact on support procedures (eg impact of taking equipment offline for maintenance)
Support	Interaction with other agencies	✓	Need to obtain support from the national support base within Australia and overseas. Need to obtain support and exchange information with other Government and international agencies – likely to become more important if Australia moves to adopt a whole-of-nation approach to Defence.
Support	Intelligence	✓	Consider new intelligence models (eg distributed analysis, burden-sharing)
Support	Research and development	✓	Include NCW-related studies
Support	Administrative & transportation	×	
Command & Management	Regulations, instructions, publications, directions, requirements, doctrine, tactical-level procedures, preparedness documents	✓	Doctrine, decision-making processes, tactical-level procedures and risk management need to support NCW tenets (eg self-synchronisation)

Appendix H: Other NCW Compliance Components

Further work is required to complete the NCW Compliance Process model. So far, only four out of seven proposed NCW Compliance components have been developed. The focus so far has been on checking projects for Net-readiness, but the NCW Compliance process will also need to assess the performance of projects within a Netforce environment.

Developing the NCW Assessment components will require further development of the top two layers of the NCW Enterprise model (Figure 1) to define an operational model and a functions and services model for the future Netforce. This will include further work to identify Netforce system-of-systems (SOS) features. This work is fundamental to understanding the Netforce and therefore to developing any NCW compliance and assessment process. Operational analysis is required to derive (from doctrine) the salient net-centric attributes for an Australian Netforce. Systems analysis is required to develop the SOS properties and functional design attributes (also known as the architectural characteristics) for the Netforce, to enable compliance checking beyond the net readiness stage.

It is envisaged that testing and assessment of system behaviour within a Netforce environment will require the following NCW Compliance components to be developed:

- NCW Linkage and Information Exchange
- Netforce Design
- NCW Experimentation, T&E.

H.1. NCW Linkage and Information Exchange

The NCW Linkage and Information Exchange component will identify legacy and future systems that need to exchange information with the program under assessment. This information should be available in the project's DAF architectural descriptions as mandated by the OCIO and maintained within an established data model employing a prescribed CASE tool. These checks will provide the system and architectural context for assessing the NCW functions and services behaviour when the program is introduced (integrated) into the Netforce. This component could also be used to prioritise legacy systems for which a wrapper should be developed to enable interfacing to the Netforce.

H.2. NCW Design

As discussed in Appendix A.2, a Netforce system-of-systems model or *Netforce Design* would identify the architecture, characteristics and functional design attributes of a future Australian Netforce. It would include a generic NCW functions and services model (probably based around the commander's sense-decide-act cycle [Polk 2000]). The NCW Design Component will be used to ensure that projects are consistent with endorsed Netforce design attributes – eg architecturally and functionally consistent.

H.3. NCW Experimentation, Test and Evaluation

NCW Experimentation and T&E checks will be used to test and assess the project's behaviour in a Netforce environment. This will include assessing its capability to exchange information with the systems identified in the NCW Linkage and Information Exchange checks. Modelling and simulation will provide an initial assessment of the behaviour of the project once integrated into its environment and experimentation will provide further data and verification of expected outcomes.

NCW Experimentation and T&E checks will be closely associated with the DMO qualification and acceptance testing process. They will therefore need to be developed in consultation with DMO. The objective will be to enable DMO to assess the project's net-centric characteristics, once it is integrated into its Netforce environment. Note that the NCW T&E component is likely to include tests that relate specifically to each of the Net-readiness Compliance components. For example there are likely to be specific tests of any security measures identified in the FIC checks.

DISTRIBUTION LIST

"As per the Research Library's *Policy on electronic distribution of official series reports* (http://web-vic.dsto.defence.gov.au/workareas/library/aboutrl/roles&policies/mission.htm) Unclassified (both Public Release and Limited), xxx-in-confidence and Restricted reports and their document data sheets will be sent by email through DRN to all recipients with Australian defence email accounts who are on the distribution list apart from the author(s) and the task sponsor(s). Other addressees and Libraries and Archives will also receive hardcopies."

An NCW Compliance Process for Australian Defence

Michele Knight, Les Vencel and Terry Moon

AUSTRALIA

DEFENCE ORGANISATION	**No. of copies**
Task Sponsor - DNCWPO	
	1 Printed
S&T Program	
Chief Defence Scientist	1
Deputy Chief Defence Scientist Policy	1
AS Science Corporate Management	1
Director General Science Policy Development	1
Counsellor Defence Science, London	Doc Data Sheet
Counsellor Defence Science, Washington	Doc Data Sheet
Scientific Adviser to MRDC, Thailand	Doc Data Sheet
Scientific Adviser Joint	1
Navy Scientific Adviser	Doc Data Sheet
Scientific Adviser – Army	Doc Data Sheet
Air Force Scientific Adviser	Doc Data Sheet
Scientific Adviser to the DMO	1
Geoff Lawrie, AOD	1
Mark Unewisse, LOD	1
Chief of Intelligence, Surveillance and Reconnaissance Division	Doc Data Sht & Dist List
Research Leader Information Integration	Doc Data Sht & Dist List
Author(s):	
Michele Knight, ISRD	1 Printed
Les Vencel, DSTO Contractor	1 Printed
Terry Moon, DSAD	1 Printed

Tim McKenna, CDSAD	Doc Data Sht & Dist List
Robert Mun, DSAD	1
Gina Kingston, DSAD	1
Åse Jakobsson, DSAD	1
Leung Chim, DSAD	1
Gary Bulluss, DSAD	1
Elizabeth Sweetman, ISRD	1
Dr John O'Neill, Head Studies Guidance Group, DSTO	1
Ruth Gani, DSAD	1

DSTO Library and Archives

Library Edinburgh	2 printed
Defence Archives	1 printed
Library Canberra	Doc Data Sheet

Capability Development Group

Director General Maritime Development	Doc Data Sheet
Director General Capability and Plans	Doc Data Sheet
Assistant Secretary Investment Analysis	Doc Data Sheet
Director Capability Plans and Programming	Doc Data Sheet

Chief Information Officer Group

Director General Australian Defence Simulation Office	Doc Data Sheet
AS Information Strategy and Futures	Doc Data Sheet
Director General Information Services	Doc Data Sheet

Strategy Group

Assistant Secretary Strategic Planning	Doc Data Sheet
Assistant Secretary Governance and Counter-Proliferation	Doc Data Sheet

Navy

Maritime Operational Analysis Centre, Building 89/90 Garden Island Sydney NSW	Doc Data Sht & Dist List
Deputy Director (Operations)	
Deputy Director (Analysis)	
Director General Navy Capability, Performance and Plans, Navy Headquarters	Doc Data Sheet
Director General Navy Strategic Policy and Futures, Navy Headquarters	Doc Data Sheet

Air Force

SO (Science) - Headquarters Air Combat Group, RAAF Base, Williamtown NSW 2314	Doc Data Sht & Exec Summary

Army

ABCA National Standardisation Officer Land Warfare Development Sector, Puckapunyal	e-mailed Doc Data Sheet
SO (Science) - Land Headquarters (LHQ), Victoria Barracks NSW	Doc Data Sht & Exec Summary
SO (Science), Deployable Joint Force Headquarters (DJFHQ) (L), Enoggera QLD	Doc Data Sheet

Joint Operations Command

Director General Joint Operations	Doc Data Sheet
Chief of Staff Headquarters Joint Operations Command	Doc Data Sheet
Commandant ADF Warfare Centre	Doc Data Sheet
Director General Strategic Logistics	Doc Data Sheet
COS Australian Defence College	Doc Data Sheet

Intelligence and Security Group

AS Concepts, Capability and Resources	1
DGSTA , Defence Intelligence Organisation	1
Manager, Information Centre, Defence Intelligence Organisation	1
Director Advanced Capabilities	Doc Data Sheet

Defence Materiel Organisation

Deputy CEO	Doc Data Sheet
Head Aerospace Systems Division	Doc Data Sheet
Head Maritime Systems Division	Doc Data Sheet
Program Manager Air Warfare Destroyer	Doc Data Sheet
Guided Weapon & Explosive Ordnance Branch (GWEO)	Doc Data Sheet
CDR Joint Logistics Command	Doc Data Sheet
Graham Eveille, Director General Electronic Systems Integration	1

OTHER ORGANISATIONS

National Library of Australia	1
NASA (Canberra)	1
Library of New South Wales	1
Gary Potts, BAES NCW/Systems Analysis Manager, BAE Systems, Taranaki Road, Edinburgh Parks, EDINBURGH SA 5111, Email: gary.potts@baesystems.com	1

UNIVERSITIES AND COLLEGES

Australian Defence Force Academy

Library	1
Head of Aerospace and Mechanical Engineering	1
Hargrave Library, Monash University	Doc Data Sheet

OUTSIDE AUSTRALIA

INTERNATIONAL DEFENCE INFORMATION CENTRES

US Defense Technical Information Center	1
UK Dstl Knowledge Services	1
Canada Defence Research Directorate R&D Knowledge & Information Management (DRDKIM)	1
NZ Defence Information Centre	1

ABSTRACTING AND INFORMATION ORGANISATIONS

Library, Chemical Abstracts Reference Service	1
Engineering Societies Library, US	1
Materials Information, Cambridge Scientific Abstracts, US	1
Documents Librarian, The Center for Research Libraries, US	1

SPARES	5 Printed

Total number of copies: 46 **Printed: 12** **PDF: 34**

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION
DOCUMENT CONTROL DATA

1. PRIVACY MARKING/CAVEAT (OF DOCUMENT)

2. TITLE

A Network Centric Warfare (NCW) Compliance Process for Australian Defence

3. SECURITY CLASSIFICATION (FOR UNCLASSIFIED REPORTS THAT ARE LIMITED RELEASE USE (L) NEXT TO DOCUMENT CLASSIFICATION)

Document (U)
Title (U)
Abstract (U)

4. AUTHOR(S)

Michele Knight, Les Vencel and Terry Moon

5. CORPORATE AUTHOR

DSTO
PO Box 1500
Edinburgh South Australia 5111 Australia

6a. DSTO NUMBER	6b. AR NUMBER	6c. TYPE OF REPORT	7. DOCUMENT DATE
DSTO-TR-1928	AR-013-770	Technical Report	August 2006

8. FILE NUMBER	9. TASK NUMBER	10. TASK SPONSOR	11. NO. OF PAGES	12. NO. OF REFERENCES
2006/1062737/1	LRR 05/014	NCWPO	68	21

13. DOWNGRADING/DELIMITING INSTRUCTIONS

To be reviewed three years after date of publication

14. RELEASE AUTHORITY

Chief, ISRD

15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT

Approved for Public Release

OVERSEAS ENQUIRIES OUTSIDE STATED LIMITATIONS SHOULD BE REFERRED THROUGH DOCUMENT EXCHANGE, PO BOX 1500, EDINBURGH, SA 5111

16. DELIBERATE ANNOUNCEMENT

No Limitations

17. CITATION IN OTHER DOCUMENTS Yes

18. DSTO Research Library Thesaurus

Network centric warfare
Capability development
Compliance
Australian Defence Force

19. ABSTRACT

The NCW Program Office (NCWPO) is responsible for ensuring that the ADF's capability projects are Network Centric Warfare (NCW) compliant, from the time they are listed in the DCP until they enter service as realised capabilities and throughout life-of-type. The NCWPO has engaged a number of different groups to look at the problem of NCW Compliance from different perspectives. This report describes one of these studies. It proposes an NCW Compliance Process that is based on a simple underlying conceptual model. It also identifies some critical issues to be addressed by the NCWPO in order to improve the rigour and quality of the NCW Compliance Process.